

Achieving safety and security in an age of disruption and distrust

Why collaboration between the public and private sectors is a prerequisite for a safe, secure and prosperous society



Contents

Foreword	2
Executive summary	3
Achieving safety and security in an age of disruption and distrust: A collaborative approach	7
What do we mean by 'security'?	7
Who's responsible?	8
Adapting to build a safer society: A systemic model of security built on trust	9
– Physical security	12
– Digital security	13
– Economic security	15
– Social security	17
– Trust	19
An agenda for action: For government	22
An agenda for action: For business and non-profits	24



Foreword

Peter van Uhm

Former Chief of Defence of the
Armed Forces of the Netherlands

In my career spanning more than 35 years working in defence, it has become increasingly clear that delivering the safety and security that citizens and businesses need to prosper requires ever closer collaborations across borders, sectors and institutions.

I learnt that rebuilding a failed state means realising that everything in a nation is interlinked and that it is all about the hearts and minds of the people. If you want the people to have trust in their society and faith in their future, safety and security in the broadest terms are the prerequisite.

To reach this prerequisite, all segments of society are important. So you need an integral, systematic approach if you want to be effective. But would this apply only for failed states, or is it also applicable to our home countries? In my opinion, such an approach is essential for every society. The real question is how to realise it.

Executive summary

Citizens and businesses want to feel safe — protected from danger, risk or injury.¹ The notion of security — commonly defined as the state of being free from danger or threat² — is therefore intertwined with safety.

The purpose of this paper is to set out some of the key challenges facing the leaders of organisations responsible for delivering safety and security in its many forms. These include traditional defence, intelligence and policing roles but go beyond that. We propose a more inclusive approach to collaboration across the public and private sectors, and across borders, to achieve a safer, more secure society. And it underscores the need to act now by highlighting case studies that illustrate how lessons can be learnt. We challenge leaders to assess what they are doing and how their actions can be augmented and strengthened to meet their citizens' needs for a more secure future.

Safety and security lie at the heart of any nation's prosperity.

The notion of security applies to anything we would want to make 'secure' from a perceived risk or threat. This includes digital and data security, national security, border security, food security, water security and social security, to name a few. All these are interconnected. In broader terms, therefore, security can be defined as the "alleviation of threats to cherished values."³

Yet today, security is being challenged in many dimensions, including physical, digital and economic. Accepted social norms of behaviour also are being challenged. Added to this is deteriorating trust in public institutions and in leaders who should be a primary source of safety for citizens and businesses.⁴ Governance is becoming increasingly difficult, and national and international unity are becoming harder to achieve.⁵ As a result, even in stable countries, many citizens say they perceive themselves to be unsafe,⁶ and businesses face their own security concerns, too.⁷

In this new reality, security, broadly defined, needs to be front and centre of government agendas — nationally, regionally and locally at the municipal level, as well as internationally — to deliver solutions that make the world a more secure place, so people trust institutions and the services they provide and so they both feel and are safe. Given that the threats come from many areas, this will require a much higher level of collaboration than we see today, both within government departments and among governments. Traditional security services such as the police, intelligence agencies and defence organisations will need to work with non-governmental organisations, businesses and citizens. With so many factors influencing perceptions of security, this type of collaboration needs a breadth of vision that is too often lacking and a level of organisational expertise that challenges current ways of working.

**Safety and security
lie at the heart of any
nation's prosperity.**



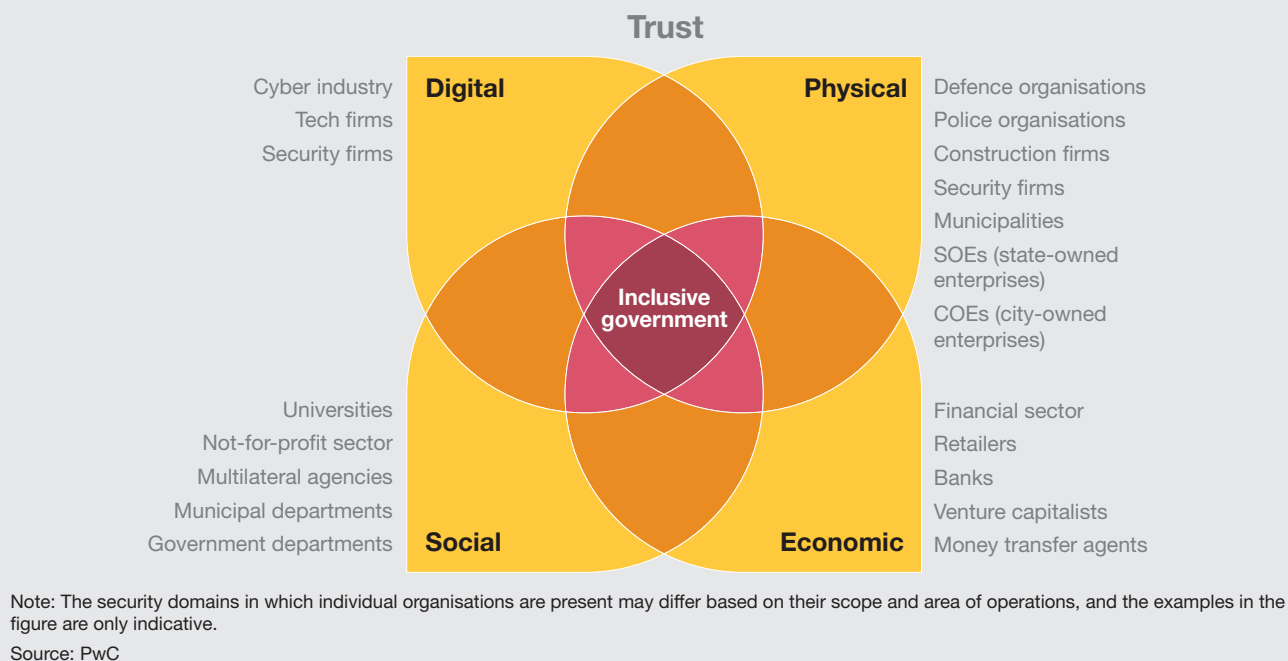
In our view, governments need to concentrate on developing systemic safety and security strategies across the public and private sectors. Leaders in a variety of institutions and organisations need to work together across interconnected areas of responsibility and take actions that make people feel more secure. When they are both believed and seen to be doing this effectively, they will succeed in delivering a more secure and resilient society that can cope with unexpected shocks and in winning back trust in the institutions that are too often seen to be letting down citizens.

A systemic approach to security, with trust and collaboration at its heart

To this end, our approach to security is purposefully broad and inclusive, with collaboration deeply embedded across four interrelated areas (see Figure 1):

- **Physical security:** The physical and institutional security of the state or territory and its administrative apparatus — the classical dimension of national security — and defence.
- **Digital security:** The protection of data and digital networked assets, regardless of whether they are owned by the state, corporations or private individuals.
- **Economic security:** The safeguarding of financial stability, nationally and within the wider global financial system. For the individual, this means, at a minimum, having enough to live on and pay the bills.
- **Social security:** Protection of citizen rights and civil liberties as traditionally defined in each state or territory. This is wider than social security as defined by a typical welfare system, including benefits and pensions; it includes food and water security, environmental sustainability, education and health.

Figure 1: Collaboration across domains to win back trust



For these building blocks to come together, they need to be built on a foundation of **trust**. Each country and each situation may require different emphasis, but the foundations of trust must be established across institutions and — in areas such as security, defence and intelligence — across borders, too.

These domains overlap and impact each other, which adds to the complexity of delivering security and the need to think holistically across all domains. For instance, economic security in a networked world is intertwined with digital security to protect against cyberattacks and data theft. Similarly, the operation of critical infrastructure is not only an issue of physical security but increasingly requires digital security, too, with a need for collaboration across organisations spanning construction to technology.

Indeed, any organisation can be — and often is — involved in more than one domain, which adds to the challenge of thinking and acting systematically in response to threats. For example, energy, utility and telecoms companies operate across all of the domains to some degree, as do health services providers whether they are private or public.

Organisations that may not have worked together in the past will need to collaborate in the future. Unless these domains are in appropriate balance and people trust their institutions and the organisations those institutions work with on a transnational basis, citizens and businesses won't be safe and secure.

Agenda for action

Making this systemic approach to security work requires specific actions. To illustrate how to put this model into effect, in this report we first discuss the foundations of security and why collaboration is required, drawing on case studies to illustrate how collaboration works in the four intersecting security domains. These real-world examples include anti-terrorist scenario planning between local and national forces in Sweden, cybersecurity defence strategies in Australia, an approach in Luxembourg to upskill workers to avoid the financial and human costs of wide-scale layoffs, the use of blockchain to secure land ownership records in India, and transnational networks to tackle food security globally.

Based on our experience, we have identified six key actions that government leaders at all levels — federal, state and local — need to prioritise now:

Six actions for government leaders

06

Manage carefully the trade-off of security with citizens' rights.
This means agreeing to a new relationship between citizens and the state in a way that safeguards an individual's personal data.

04

Develop the capacity and capability to deliver security by having distributed leadership — people empowered to make decisions — in place across the key stakeholders and sectors.

02

Identify the stakeholders needed to **collaborate to develop a joint agenda** and a national safety and security policy that can cascade to the local level, adopting an **inclusive approach to stakeholder engagement**.

03

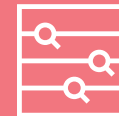
Identify exactly what each stakeholder needs to provide — for example, backup power or technical support — and **assess the level of interconnectedness** of those who need to be involved, including their critical functions and the infrastructure needed to deliver safety and security.

05

Invest in leadership to understand better how to engage the public and instil trust in the people and the organisations that serve them.

01

Develop approaches to security that are systemic, addressing the interplay of the physical, digital, economic and social aspects and spotting weak links across sectors.



Private-sector firms, from multinationals to small companies, and the not-for-profit sector (including civil society) need to address their own set of overlapping challenges:

Actions for business and not-for-profit sectors

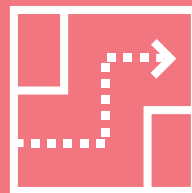
01

Work more closely with trusted governments, reviewing how the organisation engages with government on physical, digital, economic and social security.



03

Develop the capacity and capability to improve safety and security for stakeholders based on a **collaborative, cross-sector approach** that encourages distributed leadership.



02

Contribute to building trust and confidence by aligning relevant parts of the organisation's purpose to the broader societal safety and security agenda.





Achieving safety and security in an age of disruption and distrust: A collaborative approach

What do we mean by 'security'?

Security can be applied to anything we would want to protect from a perceived risk. This includes, but is not limited to, digital, national, border and social security and their interplay. In this paper, we favour the definition of security as the “**alleviation of threats to cherished values**,”⁸ with safety the desired outcome.

Nations develop because of the presence of the basic institutional elements that produce an environment in which economic and other conditions are broadly favourable to growth and prosperity.⁹ Protection of property, rule of law and the ability to uphold contracts, coupled with access to education, a relatively open market for business and broad political participation, mean that life becomes more predictable and offers more opportunity for prosperity. Transparent processes and accountable institutions that people understand foster trust and add to a feeling of safety.

If a nation can create these conditions, its citizens can feel safer and more secure to go about their lives and business in peace. However, if they cannot and prosperity is threatened by the risks and threats we discuss in this report, there will be a direct impact on security.



Interconnectedness and collaboration among key stakeholders can make a difference to delivering security in a way that no single organisation can manage on its own.



Who's responsible?

The risks and threats that citizens face have few boundaries. The actions of one individual, group or nation can have far-reaching consequences. It would be easy to discuss security with reference only to those organisations that have direct responsibility for security services, such as the armed forces, police and intelligence agencies.

But this would neglect the vast range of other public- and private-sector organisations that have an impact on delivering a more secure society. While organisations at the 'sharp end' of security are key — the police and armed forces, for example — many firms and organisations in other sectors support the sharp end by performing critical functions and/or owning and maintaining critical infrastructure.

For example, in the wider public sector, such enabling organisations include educational establishments, which have a responsibility to keep their students secure and teach them how to be safe in society; health organisations, which keep people well and safe from harm; emergency services, which respond to crises; and

employment offices, which help people find jobs and economic security. Often at the centre of these agencies are local government and city managers responsible for delivering safety and security in their communities.

In the private sector, enabling organisations include all types of businesses that are contracted to provide government services across sectors from healthcare to prison systems. They also include those that need to provide safe environments for work and those that possess confidential data that has to be stored securely. These organisations touch the supply chains for essential products and services such as energy, transport and telecommunications. In addition, particular categories of business have wider significance — for example, technology companies, which have a major impact on the security of citizens and businesses online.

These many stakeholders need to be able to work systematically together to support the wider effort to achieve safety and security. This means first identifying where an organisation fits in the interconnected ecosystem and who its key players are. The next step is strengthening relationships across sectors and enabling

those in the wider security value chain to understand their critical support functions and how they can interact to achieve security. This in turn requires organisations and institutions to operate in an environment of trust and cooperation.

It is this interconnectedness and collaboration among key stakeholders that can make a difference in delivering security in a way that no single organisation can manage on its own. More regulations are coming into effect across the globe, particularly related to data security and personal information, but this is still piecemeal. How multinational corporations and institutions that operate across borders fit into the wider security ecosystem remains unclear, resulting in a fragmented response to upholding the values that each society cherishes.

For the most part, governments uniquely have the power to facilitate and enable collaboration — whether internationally, nationally or locally — in an inclusive way across sectors of society. Their first responsibility is to identify and prioritise the threats that endanger their citizens' security.

Adapting to build a safer society: A systemic model of security built on trust

Governments, their agencies and other stakeholders need to be constantly vigilant to the risks to their citizens' safety. This means scanning the trends and assessing the threat levels and risks across the four intersecting domains of **physical, digital, economic** and **social** security.

It helps to consider these domains within the context of PwC's [ADAPT framework](#), which identifies five global issues facing the world today. Among them is trust, the overarching context in which we discuss safety and security in this report.

- **Asymmetry:** Increasing wealth disparity and the erosion of the middle class. A severely unequal distribution of wealth may ultimately lead to social unrest within countries and geopolitical tensions in and between territories.
- **Disruption:** The rise of the Internet and the spread of digital technology has resulted in a much more interconnected world, disrupted business models and blurred industry boundaries. It has empowered anyone with an Internet connection to start a business, broadcast messages, promote activism or foment social unrest. Indeed, cyberattack is among the top five threats identified by chief executives in [PwC's 22nd Annual Global CEO Survey](#), and for heads of government organisations, cyber threats rank in the top three.¹⁰
- **Age:** Demographic pressure on businesses, social institutions and economies. For instance, growing and aging urban populations challenge the resilience of critical infrastructure and those responsible for enforcing the rule of law. These challenges are accentuated in towns and cities where there are large population influxes from rural areas or neighbouring conflict zones.
- **Populism:** Breakdown in global consensus and the rise of nationalism. The shift of economic power means that new strategic geographical zones emerge and new frictions can arise between states, or between groups within states. For example, even as the middle class is growing in the developing world, it is shrinking in developed countries, fomenting discontent. Consequently, migration presents greater challenges for border control. According to Eurobarometer,¹¹ the top concern for EU citizens continues to be immigration.
- **Trust:** Declining confidence in institutions and technology. Public institutions and leaders should be a primary source of safety for citizens and businesses. But according to the international Edelman Trust Barometer 2019, fewer than half of respondents had trust in government, a level that has remained relatively unchanged for the past five years.¹²





Our approach to security is predicated on the effects these megatrends are having on society, which is why we advocate collaboration, focussed on where the key elements of ‘hard’ and ‘soft’ security overlap. This framework has to be underpinned by trust because trust gives public institutions the legitimacy to lead multi-agency responses and ensure the necessary collaboration among governments at all levels and private and not-for-profit partners.

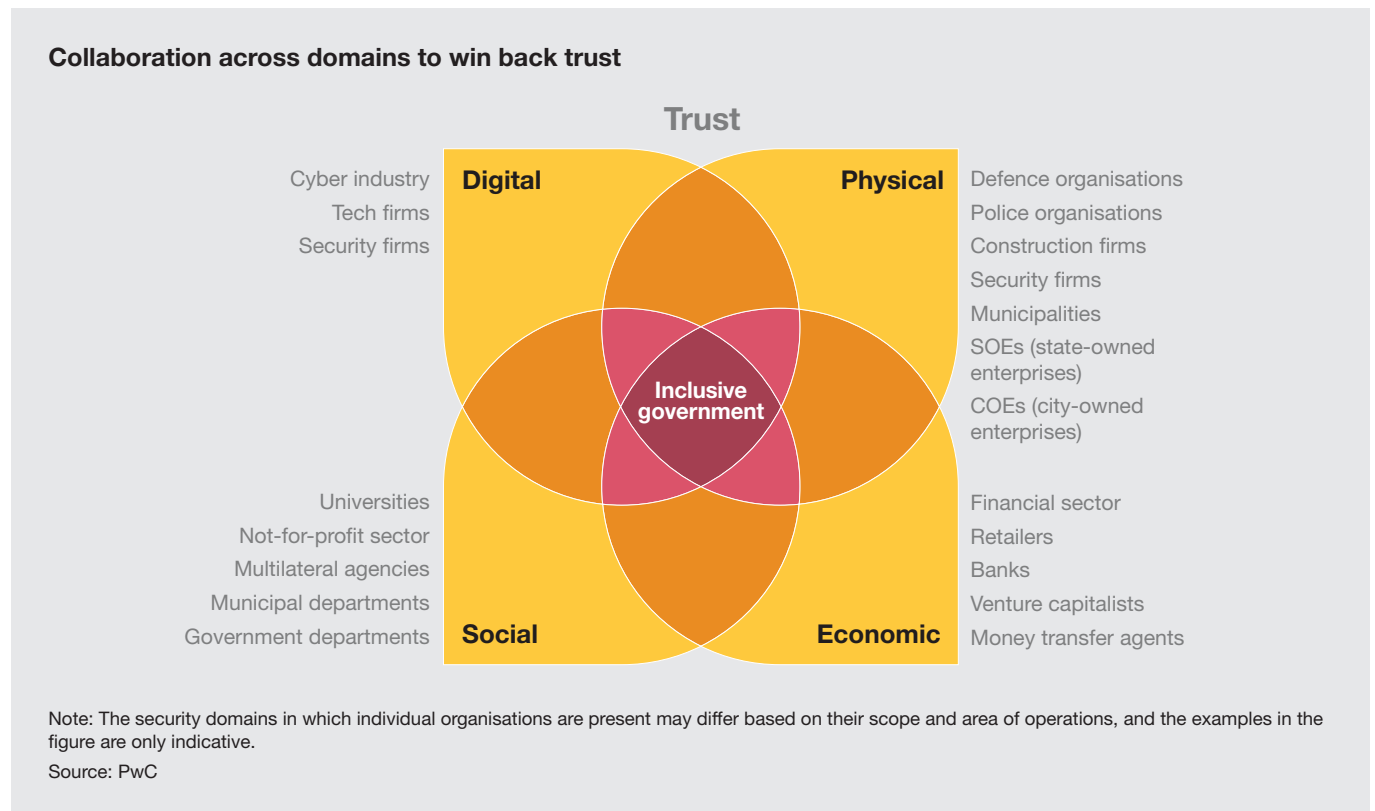
The hard aspects of security, such as size and strength of defence forces, capabilities of weapons, numbers of police officers and effectiveness of digital firewalls, can be quantitatively assessed. Soft aspects are less easy to map though just as important. They include such qualitative intangibles as political culture, the resilience and maturity of civil society, and judicial mechanisms to settle disputes, in addition to citizens’ perceptions of trust.

Both hard and soft elements interact with and influence each other. For example, installing surveillance cameras can help push down crime rates in criminal ‘hot spots,’ but it does not address the root causes of crime, which could include health issues, such as the illicit use of drugs, poverty and a faltering public education system. Installing surveillance cameras may also be seen to encroach on privacy, meaning that citizens, if they do not trust the agencies in charge of the technology, may feel less secure. Because of this, the actions to address these issues need to cross sectors and be steered by the political programmes of government at all levels, the values of key decision makers and the capacity and capability to collaborate effectively across organisational boundaries.

At the same time, security cannot solely be seen in a structural or institutional sense. For security to make sense to citizens in a broader context and to legitimise the state as the guarantor of citizen security, there is also a need to recognise the importance of trust and the influence of the social and economic domains of society.

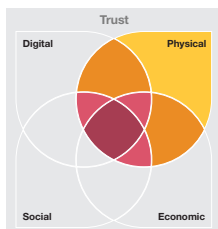
Across the world, PwC has encountered areas where successful collaborations between governments and their private and not-for-profit partners can be forged. This illustrates that it is both possible and imperative to work across each of the different domains, bearing in mind the importance of building and maintaining citizens' trust (see "Collaboration across domains to win back trust").

Below are expanded definitions of the security model's component parts, with examples of the roles different actors can play to enhance citizen security.



It is both possible and imperative to work across each of the four domains, bearing in mind the importance of building and maintaining citizens' trust.





Physical security

From a national security standpoint, the physical and institutional security of the state's territory and its administrative apparatus is the classical dimension of security. It includes the defence forces and the intelligence and policing organisations. These focus on safeguarding borders, ensuring orderly migration, protecting against military threats (including espionage) and, where necessary, projecting military power. It also means ensuring the physical security of critical infrastructure, whether it is managed by national, regional or local agencies.

In addition, physical security refers both to the protection of different — sometimes persecuted — groups and to providing post-traumatic psychological assistance to the individual.

In recent years, physical security has extended to managing crises. For instance, climate change affects the environment and may cause natural disasters on an unprecedented scale. Indeed, in the UK, the 2018 National Security Capability Review identified disease and natural hazards as one of the six major challenges facing UK security.¹³ Managing crises requires government action to deal with, for instance, disruption to critical infrastructure such as transportation, power and other utilities. It also means making society more resilient to events, including those caused by terrorist attacks (see: “Crisis readiness: Stockholm terrorist attack, 2017”).

Government's role is to build more risk-resilient infrastructure to deal with threats to security and to lead a whole community response where planning takes place before disasters occur. This requires public-private collaboration because the private sector delivers many of the services that might be at risk. A holistic strategy will make communities more resilient and better able to return to their primary functions after a disaster.



Crisis readiness:

Stockholm terrorist attack, 2017

At the beginning of 2017, PwC worked with one of Sweden's most important and largest regional governing bodies, the County Council, to strengthen its crisis readiness and management capability. This involved training the political leadership to increase awareness about the tasks, assignments and the authority under which politicians can operate in times of crisis. The assignment included the use of scenario planning, such as a terrorist attack in the central part of Stockholm.

Sadly, on April 7, 2017, an attack occurred, when a lone wolf stole a truck and drove at high speed into a crowded pedestrian street, resulting in five casualties and a number of people being severely injured. In response to the event, the emergency health services went on highest alert and the public transportation system was shut down. The scenario-planning exercise carried out just months before the attack is likely to have strengthened the organisational capability to handle the crisis as it happened.

About a week after the attack, the County Council asked PwC to assist with expertise to the council's evaluation of its efforts related to the terrorist attack and suggest further improvements. PwC contributed with expert competencies in crisis management for the council's evaluation team. The majority of the proposals that the evaluation/investigation came up with on how to promote collaboration between agencies and improve lines of communication were accepted.

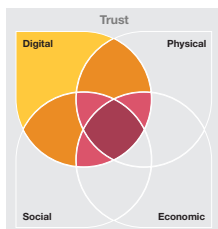
Lessons learnt: The importance of politicians and officials having joint awareness of their roles and responsibilities in an organisational crisis; developing and maintaining an ongoing process for strengthening and improving their crisis readiness; and stress testing this through scenario planning.



Physical security: Questions to think about

- Q. Who are the key stakeholders you need to collaborate with to deliver physical security in your area and beyond your boundaries?
- Q. How well developed are your relationships with these other organisations to deal with threats, including natural disasters, and plan to manage crises?
- Q. What more can you do to ensure that critical functions are delivered effectively and that critical infrastructure is risk-resilient and within your scope of influence or control?





Digital security

Emerging as a vital building block of societal trust in recent years, digital security covers issues related to the protection of digital and networked assets. These include personal data, regardless of whether it is owned by government (e.g., social security numbers and patient data), by corporations or not-for-profit organisations (e.g., financial records, intellectual property and employee data) or by private individuals (e.g., biometric data).

Those seeking to illegitimately acquire digital assets and personal data target the private and public sectors as well as individuals. They can be non-state operatives or those acting on behalf of a state who seek to disrupt services such as energy, water, communications or other critical infrastructure. Indeed, hybrid warfare — a combination of traditional military and cyberattacks — has become part of the everyday activities of states and other agents for which information or disinformation ('fake news' or 'alternative facts') has become weaponised.

The lack of international governance over these areas has created the opportunity for nation-states to seek influence by both indirect and informal actions — for example, through the use of illegally accessed personal data and the deployment of bots by foreign governments to manipulate and influence national elections.

In addition, organised crime and terrorist groups are becoming more sophisticated in cybercrime and, for the latter, in developing propaganda campaigns. The cost for entry is low, the risk of detection may be negligible and the likelihood of being held accountable in any international sense can be virtually zero. That makes cybercrime and propaganda efficient ways for agents to obtain money or information (industrial espionage), disrupt services (sabotage) or influence public opinion.

The effects are significant. By 2022, it's estimated that companies will spend US\$1tn globally to protect themselves from cybercrime, far more than the record US\$300bn of damage due to natural disasters in 2017.¹⁴ The cyber domain is largely ungoverned and operated without broadly accepted norms.¹⁵ Cross-national agreements are limited to security frameworks and risk models and to a few cases of multilateral government cooperation on cyber defence.¹⁶

Moreover, approximately 90% of cyberspace resides in the private sector. This essentially means that the vast majority of cyber infrastructure and operations have been designed, developed and put into operation with limited government involvement.¹⁷ An attack against private cyber infrastructure may therefore turn into a threat against national security. Indeed, 72% of CEOs surveyed say their company could be hurt by geopolitical cyber activity.¹⁸ As global tensions rise, more companies could be targeted by, or suffer

An attack against private cyber infrastructure may turn into a threat against national security.





Spotlight on cyber threats:

Cloud Hopper

collateral damage from, operations launched by state-sponsored hackers. Yet relatively few CEOs have strong confidence that key cyber and privacy risk management outcomes are being achieved.

The lack of a unified approach to tackling cybercrime complicates government's ability to map the risk and threat environment and take the necessary actions to withstand and deter attacks. It also makes it harder to draw the line between the responsibility of government and the responsibility of the private sector. More collaboration is essential (see: "Spotlight on cyber threats: Cloud Hopper").

Alongside the more obvious threats from malign actors, digital security also includes the individual's right to privacy and confidentiality, and the ethics surrounding the use of personal data. This is critical to fostering public trust. This is not just a matter of stealing credit card details. There are more profound issues that may require difficult trade-offs between information sharing and subsequent benefits to society. For example, data analytics can further the understanding of disease management and improve public health using personal data. But what this could mean on the individual level — in terms of health insurance or access to capital for people — requires detailed and inclusive discussions.

There are profound issues that may require difficult trade-offs between information sharing and subsequent benefits to society.

In April 2017, PwC UK uncovered an unprecedented but highly effective cyber espionage technique during an ongoing project to monitor computer network security.¹⁹ The perpetrators sought to steal sensitive intellectual property and personal data from businesses in at least 14 countries by spreading a computer virus. They had hacked the systems via third-party IT service providers. The action was code-named Cloud Hopper.

After the hack was discovered, PwC collaborated with a team of threat intelligence experts from the private sector, the security community and government to understand how the hacker had compromised the system and to disrupt further attempts at stealing data. It was an example of close public- and private-sector collaboration.

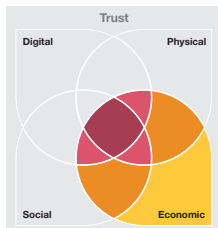
Lessons learnt: Forging strong collaboration with members of the cybersecurity community, both in the public and private sectors, was invaluable in identifying and neutralising a threat that targeted the supply chain through third-party providers. It highlights the need to ensure that all third-party contracts and service level agreements encapsulate a minimum acceptable standard for security policy and the need to share information. This can pre-empt future damage, for example, by limiting access to systems and segmenting business networks so that valuable information cannot be obtained directly.



Digital security: Questions to think about

- Q. Which key stakeholders do you need to work with to deliver digital security?
- Q. How well developed are public-private relationships to deal with cyber threats and ensure that your digital infrastructure is risk-resilient?
- Q. What trade-offs are needed to balance individual confidentiality with valuable data sharing? What is the role of regulation, and who should draft the rules?





Economic security

The interconnected global economy is at the heart of delivering economic security, and maintaining it requires an ever changing cast of players to interact. These players need to work together to safeguard the financial stability and integrity of the nation-state while, across borders, also safeguarding the wider global financial system and intellectual property and minimising the threat of interference in financial markets. This is done through continued fiscal discipline locally, nationally and multilaterally and cooperation among cross-border agencies skilled in fighting financial crime.

Economic security also means developing and maintaining a broadly stable macroeconomic environment and an approach to markets and competition that maintains a level playing field and encourages enterprise, growth and prosperity. In today's environment, this presents even greater challenges as the benefits of globalisation and freer trade are disputed and as some governments resort to protectionism in an attempt to secure short-term economic security.

Economic security also extends to maintaining access to basic infrastructure and basic living standards (see: "Establishing food security for citizens"). This requires government to work with the private sector to design, build, finance and operate the infrastructure and ensure the security of supply chains across borders.

Economic security includes supporting nations, especially in post-conflict situations where economic development is a key part of rebuilding failed states. This can include rebuilding public institutions and governance as well as supporting private-sector infrastructure development.

Outside the public domain, economic security is about providing an environment that is stable and predictable, and where transactions — including mergers and acquisitions and trade — are safeguarded. The rule of law and contractual fulfilment are examples of those fundamental principles that need safeguarding. This means building a trusted business environment.

The baseline for economic security of the individual requires that citizens should have sufficient income to meet basic needs, ideally with a little to spare. As we discuss in PwC's research with Demos in the UK on good growth for cities,²⁰ this means having access to jobs, education and healthcare (see: "Beyond GDP," next page).



Establishing food security for citizens

By 2050, the global population will be 35% larger than today — reaching almost 10 billion — and economic development will continue to shift diets from simple grains toward more resource-intensive sources of protein. As a result, global food production will need to double despite increasing scarcities of land, labour, water and energy. A way must be found to produce more food from fewer resources. Governments and the private sector can take steps to map out a food security strategy.²¹



Beyond GDP

If the pursuit of growth is essentially about improving the prosperity, life chances and well-being of citizens, is there more to the equation than a narrow focus on gross domestic product (GDP) or gross value added (GVA)? Our research with think tank Demos, launched in 2012, created the Good Growth for Cities Index, based on the public's views of what economic success means to them. Within the index, good growth encompasses broader measures of economic well-being, including jobs, income, health, skills, work-life balance, housing, transport infrastructure and the environment — the factors that the public has told us are most important to the work and money side of their lives.

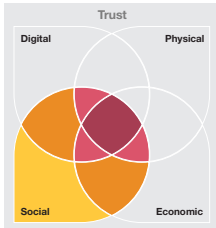
Lessons learnt: Local economic development is about policy choices and priorities — where to act and invest scarce resources to promote growth. The Demos-PwC Good Growth for Cities Index provides a framework for allocating resources and investment, in which decisions are based on what people want. This is an opportunity to move beyond the narrow confines of traditional economic measures and for city leadership to start with the outcomes that people — the voters — value, and so provide a more democratic, needs-based dimension to the decisions made.



Economic security: Questions to think about

- Q.** How well developed are the basics of economic security in your area, such as the rule of law, fiscal and budget discipline, open markets and macroeconomic stability?
- Q.** To what extent are citizens economically secure, with access to jobs that pay a living wage, and able to cope with risks to job security such as the impact of artificial intelligence and robotics?
- Q.** What more needs to be done to ensure businesses can prosper, grow and deliver the good jobs that citizens want?





Social security

A stable, secure society is a result of people living together, pursuing happiness and sharing some basic values. It involves the protection of citizens' rights or civil liberties as they have traditionally and contextually been defined in each territory, meaning that they are culturally and geographically dynamic.

For society to be legitimate and to 'make sense' to the individual as a collective with which to identify, a meaningful social contract must be in place. That contract, in turn, must depend on trust in institutions as recognised in the challenges set out above in our ADAPT model. Through this, individuals secure their basic rights and get something in return from the state: certain basic civil liberties that might include freedom of information, data protection, protection from foreign interference in internal affairs, and stable government (e.g., the protection of asset ownership, defence and the rule of law).

This includes, but is not restricted to, social security as defined by a social welfare system. It includes ensuring access to education and skills development, one of the basic institutional prerequisites for prosperity and critical to future prosperity, particularly in the new digital era (see: "Upskilling the workforce: The need for new collaborations"). Consistent with past years, in PwC's [22nd Annual Global CEO Survey](#), CEOs said they see a lack of skills as a barrier to growth. For individuals, it is a barrier to good jobs and a decent income.



Upskilling the workforce:

The need for new collaborations

In 2018, the government of Luxembourg, under the co-leadership of the ministries of labour and economy, joined forces with trade unions, trade associations and businesses to form the Luxembourg Digital Skills Bridge initiative. The goal was to create a broad coalition to help workers learn the new skills employers were looking for. The key objective was to upskill people at risk of losing their jobs because of automation and give them the opportunity to gain technical and digital skills that would enable them to take on new roles. In theory, this approach would save the government money on unemployment costs by investing in building a cluster of digitally oriented industries and developing the relevant skills in workers who might otherwise have been laid off. PwC was part of the initiative from the start.²²

This cluster-based approach required significant upfront coordination among government, unions and businesses. The initiative assembled digital apps and tools for all participants to share. Companies agreed to foster long-term employability, even if that meant investing in employees who might move to other companies in the future. Midway through the initiative, nine out of ten workers were expected to take up new roles in the company where they were currently employed. The original objective was to have 65% of the participants stay in the same company and take up new functions. The initiative covered 90% of an employee's salary during the training period, plus a portion of the company's training costs.

Lessons learnt: This proactive model illustrates the kind of collaboration needed to deliver on societal goals at a time when technological change is threatening the structure of society — in this case the labour force — in destabilising ways. Upskilling does not just teach people a few technical skills. It teaches them to take charge of their lives and provides lifelong learning opportunities, as the skills we need today will become redundant based on the innovations of tomorrow. And it requires a high level of collaboration between institutions and business.





Can blockchain solve the land ownership issue?

Social security also depends on the healthcare system to ensure that people are well enough to live, work and contribute to society. According to PwC's 2019 [Health Research Institute survey](#), one-third of respondents said they had not engaged in conversation with the full range of stakeholders who affect their health. Governments can act as conveners to help build coalitions of partners, including universities, retailers, government agencies and technology companies, to ensure that health goals and policies are aligned. Social security also means providing access to affordable housing so citizens have shelter. In the UK, housing associations play a vital role in this regard.²³

There are many challenges to ensuring these basic rights are met and needs are fulfilled. It means securing property rights and the freedom to contract and exchange assets. In many countries, asset ownership can vary over time depending on government policies, with a need to transfer assets from the state to individuals. In some countries in Africa, this has led to allegations of corruption because land registries are not secure. In India, new technology — such as blockchain — may be a way to address this issue where digital and social security overlap (see: “Can blockchain solve the land ownership issue?”).

The depth and breadth of what is included in the social contract and the need for diverse parties to work together to ensure it is functional highlights, again, the importance of well-thought-out collaboration across sectors and actors.

In India, land ownership is presumptive in nature. Various documents such as registered sale deeds, property tax documents and government surveys record rights of the title holder against claims made by another party. However, they do not always ensure the landowners a government-guaranteed conclusive title to the property.

Blockchain technology can help. It creates a tamper-proof ledger that can act as a ‘single source of truth’ for land records across various government departments. Attributes of blockchain such as immutability, provenance, finality and decentralisation make it a logical choice for storing sensitive, conclusive land-record information securely, transparently, efficiently and with enhanced verifiability.

A provincial government in India is working with PwC to define, design and later implement a blockchain titling system that will let citizens securely manage their land records and control the transactions made over it, while significantly reducing the total turnaround time from the current standards.

Lesson learnt: The conclusive titling system ensures a form of government protection and guarantee of citizens’ rights over their land, boosting trust in the land records. This could reduce litigation and arbitration over property, which accounts for about 66% of court cases in India. The final outcome is intended to be a system in which the various departments that deal with land titles would have a common, conclusive and secure view of each property, with a single place for citizens to seek services.



Social security: Questions to think about

- Q. How well are citizens’ rights protected and their responsibilities enshrined in a formal or informal social contract with the state?
- Q. To what extent is there equal access to the basic needs in life, such as food, housing, healthcare and education?
- Q. What more needs to be done to ensure that basic rights around asset ownership and transfer are enforced?



Trust

For these building blocks to come together, the underlying condition and prerequisite is trust: people need to trust in a system, an institution or someone in whom confidence or faith is placed. In an era in which fewer than half of people trust institutions, according to the Edelman Trust Barometer, the task of building or re-establishing trust is both a priority and a major challenge for leaders and their teams across organisations.

To run the economy — for example, central banking, national budgets and taxation — the executive state needs to be trusted. For the state to be able to drive the legislative process on privacy issues and digital security, and as the last guarantor of digital functionality in society, it must be trusted by both the public and by the private sectors. Finally, to manage the parts of society relating to citizens' social well-being, such as labour market regulation, social welfare, data privacy and education, or even export policy decisions, the state needs to be trusted.

One recent example in building trust across institutions is the 22 July Commission in Norway, which was set up in the wake of terrorist attacks. People needed to know how such an event could have happened, what the organisations that were supposed to keep people safe had learnt and, most importantly, what actions they were taking to make sure planned future attacks were either intercepted before they happened or neutralised quickly (see: "Rebuilding trust in the wake of the terrorist attack in Oslo").



Rebuilding trust in the wake of the terrorist attack in Oslo

The 2011 terrorist attacks in Norway, referred to in Norway as 22 July, when Anders Behring Breivik went on a rampage against the government, the civilian population and a Workers' Youth League summer camp on Utøya island, claimed the lives of 77 people.

In August 2012, the 22 July Commission presented its report on how the authorities and society at large dealt with the crisis. The report, which also discussed the underlying causes, concluded there was insufficient coordination among agencies and made recommendations about what the authorities ought to do to ensure that Norway would be better equipped to withstand attacks in future.

A team from PwC was secretariat for the commission and assisted in analysing the role of all the parties (e.g., police, healthcare, ministries of security and service organisation, ministry of justice, the Government, Oslo municipality), involved before, during and after the attack. Subsequently, we worked on a restructuring plan with the police that included an emphasis on broader communications with other authorities, including the military, and the building of a new headquarters with operational capabilities for anti-terror police.

Indeed, trust in any leader or organisation is a powerful asset and can transform citizens' views toward public- and private-sector institutions. To protect citizens and property — in particular against terrorist attacks, extreme weather events or military aggression— the defence forces and emergency services must be trusted to have the citizens' best interests at heart; people need to be able to trust them with their lives. In the case of cyber warfare and data attacks, people also need to know that the private-sector firms they entrust their data to are properly regulated and have the means to protect that information.

Equally, for citizens to trust institutions, they need to feel engaged and connected to them. Citizens need to understand the impact of threats to their security and how they can reduce their exposure to risk. This can often stem from the advice and guidance they get from these institutions. When citizens can see that they are getting valuable information and services that increase their security, their trust in these institutions increases.

PwC's research in the UK into the value and drivers of organisational trust²⁴ highlights four operational reasons for an organisation to be trustworthy: trust drives performance, it can put an organisation on the front foot in a crisis, it can overcome stakeholders' scepticism and it allows organisations to be true to themselves.

Security, freedom and prosperity are core public interests that any democratic government should bear in mind when formulating security policy. Governments ultimately make policy decisions about societal needs that are considered to be in the public interest and that are to be safeguarded by government intervention. Such intervention is required when market dynamics are expected to fall short of guaranteeing those interests. In terms of optimal allocation of public and private responsibilities, the government is ultimately responsible.

Strong institutions allow people to trust in each other, which in itself is a prerequisite for peace and security. However, while strong institutions are necessary, they are not sufficient to deliver security. Trust is built where such institutions collaborate to solve problems and are seen to do this, which means having strong links among the leaders of organisations across sectors.

Trust is built where institutions collaborate to solve problems and are seen to do this, which means having strong links among the leaders of organisations across sectors.



Trust: Questions to think about

- Q. To what extent is your organisation trusted by citizens/businesses/civil society?
- Q. Does your organisation have a clear purpose that sets out what it does and how it contributes to society?
- Q. What more needs to be done to build trust in your organisation among its key stakeholders?





Distributing leadership roles means identifying the key players across organisations who are empowered to make decisions and ensuring they collaborate with one another.

Distributed leadership and active collaboration: How to build trust

Delivering a safe and secure society depends greatly on a government's ability to lead a cross section of agencies in an inclusive way towards a common goal while safeguarding the freedom of individuals and organisations in the system. This is true at the national, regional and municipal level. It means distributing leadership roles: identifying the key players across organisations who are empowered to make decisions and ensuring they collaborate with one another. No easy task, particularly as there is also a growing need for international collaboration and capacity building to tackle controversial issues that cross borders.

Mass migration is a case in point and likely to climb higher up the political agenda as the effects of climate change, in addition to conflict, displace more populations. For example, the UN's International Organisation for Migration is attempting to bring together, on a macro level, the institutions that will need to collaborate. This is distributive leadership in action, across what we have called the penta-helix of stakeholders: public sector, private sector, non-governmental organisations, universities/knowledge institutes and citizens.

More generally, government at all levels — international, national and local — has a key leadership role to play. But it is not the only player. In so many areas of life, the behaviours and actions of private-sector businesses, academic institutions and not-for-profit organisations, as well as citizens, are outside of direct government control. The institutions and organisations that make up the penta-helix model will need to interact on a daily basis.

By working together, leaders in these organisations can create a sense of safety in society, although in many cases they do not come together as often as they should. There is an urgent need in today's world to formalise the mechanisms to make this standard practice. Doing so will also help build the capacity and capability of the broader distributed network of stakeholders whose actions keep citizens and businesses secure from the threats they face.²⁵ Government can and should lead the way. For example, the European Union sees it as a priority to enable member states to collaborate more closely with each other on security issues, including providing grants for collaborative projects — for example, the use of drones and strategic technology.

An agenda for action: For government

In PwC's 2013 report *Future of Government*, we asserted that the public body of the future needed to be citizen-centric, meaning it serves the empowered citizen.²⁶ This means both public- and private-sector bodies need to be connected to society and be transparent and accountable in order to safeguard the foundational trust upon which all meaningful human interaction depends. This holds true today even though much has changed since that report, most notably the widespread questioning of the benefits of globalisation and the subsequent rise of nationalism and populism.

In the current era of rising citizen expectations and individualism, it is tempting for governments to put in place populist policies to stay in power or for opposition parties to promote them to gain power. At the same time, the Internet is allowing citizens to hold governments to account for their actions. This greater transparency and accountability should help organisations build or rebuild trust and legitimacy in the eyes of the wider public. But it can also undermine trust when misinformation spreads virally. If society is to prosper, there is a need to protect and safeguard the very institutions and organisations that help nations thrive and protect citizens against the risks and threats we have identified. But it also means safeguarding the rights under which the citizens can make their voices heard in the first place.

This is why security, broadly defined, needs to come to the front and centre of governmental agendas, nationally, regionally, locally and internationally. In particular, government leaders at all levels need to act in six key areas:



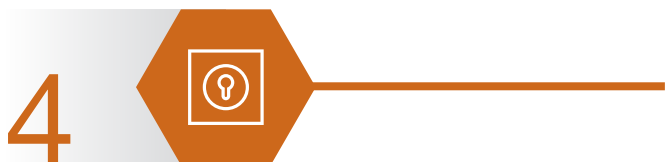
1 Develop **systemic** approaches to security. To what extent does your existing approach need to adapt to address the interplay of the different physical, digital, economic and social aspects? Also, strong lines of communication are needed across organisations, with active scenario planning to spotlight weak links across societal sectors.



2 Identify the stakeholders needed to **collaborate** to develop a joint agenda and a national safety and security policy that can cascade to the local level, adopting an **inclusive approach** to stakeholder engagement. This includes but is not limited to the traditional defence, policing and intelligence bodies. A siloed approach will not work. Only proactive mapping will identify areas of concern. How can you improve collaboration across government and with the private and not-for-profit sectors? Are you looking at the wider value chain to involve a broader group of stakeholders — for example, in energy, transport and telecommunications?



3 Identify key deliverables and **assess the interconnectedness** of those involved across sectors in their delivery. What are the critical functions and enabling infrastructure needed? Where do links need to be strengthened — for example, among those involved in crisis management?



4 Develop the **capacity and capability** to deliver safety and security, in particular by identifying whether the required **distributed leadership** is in place across sectors. At the national, state and local levels, where are the gaps in the capacity and capability to develop and implement a systemic approach to safety and security? What are the priority investments needed to fill those gaps?



5 Invest in **leadership** — particularly **distributed leadership** — to understand better how to engage the public and instil a sense of trust in those who serve them. What more can you do to rebuild trust in the institutions that can guarantee safety and security?

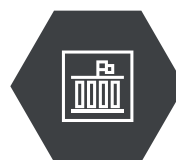


6 Manage carefully the **trade-off of security with citizens' rights**. This means agreeing to a new understanding between citizens and the state about how people's data will be safeguarded. How do behaviours and strategies for engagement with citizens need to change?



An agenda for action: For business and non-profits

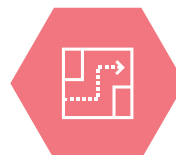
Action by government and its agencies is not sufficient to deliver the security and safety citizens desire. Private-sector firms of all sizes and the not-for-profit sector, including civil society, have essential roles to play as well and need to address their own set of overlapping challenges:



- **Work more closely with trusted governments**, reviewing how your organisation engages with government on different aspects of security: physical, digital, economic and social. How can you improve collaboration with government and its partners on security issues?



- Contribute to **building trust** by aligning relevant parts of your organisation's purpose to the broader societal safety and security agenda. What needs to be done to build trust with your stakeholders and so boost security and safety for your employees, customers, supply chain and the local communities in which you operate?



- As with government, develop the **capacity and capability** to improve safety and security for your stakeholders. What are the gaps in your capacity and capability to develop and implement a systemic approach to safety and security? What are the priority investments needed in each sphere to increase safety and security?

Achieving and delivering a national or local 'safe and secure' policy is a challenge. It will require a level of transparency and trust to enable citizens to feel comfortable that security does not overstep the mark and invade their privacy. This means understanding the choices and benefits of providing more information to improve security, which will differ around the world and at different times and will depend on trust in the organisations delivering security.

The approach has to be systemic and inclusive. Simply spending on more extensive border controls and increasingly sophisticated weapons is not enough. Societal and economic security must always be part of the equation, as must developing strategies geared to winning trust, which is the overriding goal and which is indispensable to making people feel safe and secure.

Endnotes

1. As defined in the Oxford English Dictionary.
2. As defined in the Oxford English Dictionary.
3. Paul Williams and Matt McDonald, eds., *Security Studies: An Introduction* (3rd ed., Routledge, 2018), p. 1. According to the authors, “Most scholars within international relations (IR) work with a definition of security that involves the alleviation of threats to cherished values.” This definition lets us approach security in a meaningful way on all levels of society — public, private and not-for-profit, as well as domestic and international.
4. The Edelman Trust Barometer 2019 found that only 47% of 33,000 respondents from 27 countries had trust in government: <https://www.edelman.com/trust-barometer>.
5. UK Ministry of Defence, *Global Strategic Trends (out to 2050)*, Oct. 2018: <https://www.gov.uk/government/publications/global-strategic-trends>.
6. For instance, Gallup’s 2018 *Global Law and Order Report* shows a lot of work remains to be done to achieve “a more peaceful and secure world,” particularly in places such as Afghanistan and Venezuela: <https://news.gallup.com/reports/235310/gallup-global-law-order-report-2018.aspx>.
7. PwC, *22nd Annual Global CEO Survey*, 2019: <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019/gx.html>.
8. Williams and McDonald, eds., *Security Studies: An Introduction*, p. 1.
9. There are numerous ways to measure how and why nations thrive in terms of positive economic development and quality of life for their citizens. Examples include the Human Development Index, the Legatum Institute’s Prosperity Index, the *World Happiness Report*, PwC’s Cities of Opportunity and the Demos-PwC Good Growth Index.
10. PwC, *22nd Annual Global CEO Survey*, 2019: <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019/gx.html>.
11. Eurobarometer publishes public opinion surveys for the European Parliament: <http://www.europarl.europa.eu/at-your-service/en/be-heard/eurobarometer>.
12. The Edelman Trust Barometer 2019.
13. Cabinet Office, HM Government, *National Security Capability Review*, March 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.
14. Paul Mee and Til Schuermann, “How a Cyber Attack Could Cause the Next Financial Crisis,” *Harvard Business Review*, Sept. 14, 2018: <https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis>.
15. Tarah Wheeler, “In cyberwar, there are no rules,” *Foreign Policy*, Sept. 12, 2018: <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>. See also Williams and McDonald, eds., *Security Studies: An Introduction*, p. 557.
16. One example of an ambitious and growing body of legislative exploration in this area is the Tallinn Manual, developed by the NATO Cooperative Cyber Defence Centre of Excellence, first published in 2013. The most recent edition is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017): <https://ccdcoe.org/research/tallinn-manual/>.
17. Williams and McDonald, eds., *Security Studies: An Introduction*, p. 561.
18. PwC, *22nd Annual Global CEO Survey*, 2019: <https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019/gx.html>.
19. PwC UK, “Uncovering a new sustained global cyber espionage campaign.” April 2017: <https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html>.
20. Demos-PwC, *Good Growth for Cities 2018: Measuring what matters when it comes to growth*, 2018: <https://www.pwc.co.uk/industries/government-public-sector/good-growth.html>.
21. PwC, *Feeding Ten Billion: Building a robust food security strategy*, 2017: <https://www.pwc.com/sg/en/services/food-supply-integrity/feeding-ten-billion-building-a-robust-food-security-strategy.html>.
22. Laurent Probst and Christian Scharff, “A strategist’s guide to upskilling,” *strategy+business*, July 25, 2019: <https://www.strategy-business.com/feature/A-strategists-guide-to-upskilling?gko=0bb8b>.
23. PwC, *Growth, place or people: the housing association of 2022*, 2018: <https://www.pwc.co.uk/industries/government-public-sector/local-government/insights/growth-place-or-people-the-housing-association-of-2022.html>.
24. PwC, *Understanding the value and drivers of organisational trust*, 2015: <https://www.pwc.com/my/en/assets/trust/trust-insight-understanding-the-value-and-drivers-of-organisational-trust.pdf>.
25. PwC, *iUrban: Enabling sustainable city competitiveness through distributed urban leadership*, 2016: <https://www.pwc.com/gx/en/industries/government-public-services/public-sector-research-centre/urban-leaders.html>.
26. PwC, *Future of Government: Tomorrow’s leading public body*, June 2013: https://www.pwc.com/gx/en/psrc/publications/assets/pwc_future_of_government.pdf.

Authors

**Tony Peake**

Global Leader, Government and Public Services
Partner, PwC Australia
tony.peake@pwc.com

**Egon de Haas**

Global Government and Public Services
Senior Manager, PwC Netherlands
egon.de.haas@pwc.com

**Linus Owman**

Cybersecurity
Senior Manager, PwC Sweden
linus.owman@pwc.com

Other contacts

**George Alders**

Global Government Security Network
Director, PwC Netherlands
george.alders@pwc.com

**Terry Weber**

Global Government Defence Network
Partner, PwC Australia
terry.weber@pwc.com

The authors would like to thank Nick C. Jones for his help in writing this report.

pwc.com/safe-society

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services.

Find out more and tell us what matters to you by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2019 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.