pwc.com/SEAM

Evaluating and learning from the pandemic response

Threats such as the COVID-19 pandemic test the crisis responses of public institutions, businesses and citizens. When we look back, it will become clear what governments could have done better.

pwc

Foreword

In recent decades, nations have become more sophisticated in their response to domestic and global threats, and the threats themselves have become more complex. Threat response requires a high level of collaboration between the public and private sectors that goes well beyond the role that defence and security have traditionally played in safeguarding nations.

A pandemic such as COVID-19 tests all these relationships. It shows the need for collaboration and coordination across sectors and institutions. And around the world, we are seeing traditional defence and security forces such as the army and the police, as well as private industry, stepping in to help health services and governments that are operating under immense pressure.

In this report, we look at the responses to the COVID-19 world health crisis through a defence and security lens. We use a framework that was developed by PwC specifically to identify where there may be weaknesses in working relationships within a broadly defined defence and security ecosystem, which includes both public- and private-sector institutions. In our respective fields, over the past decade, we have witnessed the need for the traditional command-and-control lines of defence and security institutions to become more agile and flexible. Only then can they effectively address the threats of the 21st century — those that already exist and those that have yet to materialise.

As parts of the world move from the immediate crisis to a more stable phase, leaders will have an opportunity to look at the ad hoc arrangements that had to be put in place to overcome weaknesses in their preparedness. They will be able to examine ways to institutionalise those actions that worked and change those that didn't and thus improve crisis resilience going forward. We believe a systematic framework such as the one described here is an important contribution to keeping citizens safe.

Malcolm Brown was Deputy Minister of Public Safety in Canada from 2016 to 2019. He is a senior strategic adviser to PwC Canada.

Craig Mackey QPM was the Deputy Commissioner of the Metropolitan Police Service in London from 2012 to 2018. He is an adviser to PwC UK.

Peter van Uhm, a retired general, was the Chief of Defence of the Netherlands from 2008 to 2012. He is an adviser to PwC Netherlands.

George Alders, of PwC's Global Government Security Network, is a director with PwC Netherlands.

Terry Weber, of PwC's Global Government Defence Network, is a partner with PwC Australia.

Introduction

In South Korea, the army helped spray disinfectant on the streets as a precaution against the coronavirus. In India, the government mobilised 28 army field hospitals to treat COVID-19 patients, and in the US, the Navy sent hospital ships to New York and Los Angeles to boost bed capacity. In Spain and France, troops enforced lockdown orders; in the UK, the military helped turn convention centres into hospitals and used their logistics skills to move supplies to the medical front lines. Canadian troops are helping out in care homes across the country, and in Australia the army is still assisting police in monitoring and enforcing social distancing and self-isolation.

Police forces around the world are reminding people to stay at home and issuing fines if they disobey local regulations. And globally, private-sector manufacturing production lines are adapting or being commandeered to produce medical supplies, including ventilators and protective clothing. Even luxury perfumeries and distillers are making hand sanitisers.

The world is on high alert against an invisible enemy that knows no boundaries. It is the plot of many works of fiction being played out in real life, watched by billions of people, 4 billion of whom are either in lockdown or just beginning to emerge from their homes months after the pandemic began. What people are experiencing is the activation of crisis response scenarios that some governments prepared as hypothetical exercises and others are scrambling to imitate.

Today, governments are broadening their national security scope by including elements of economic, health, technological, ecological, food and political security. And that complicates responses. What constitutes a threat and how to prioritise threats both depend on a country's view of national security and its defined vital interests.

In this report, we look at the interconnected relationships among the institutions that need to work together to protect citizens. For this purpose, we use PwC's Security Ecosystem Assessment Map (SEAM) model, which is a structured way of codifying the relationships that will be critical to achieving desired outcomes in the face of threats. It helps identify the

The world is on high alert against an invisible enemy that knows no boundaries.

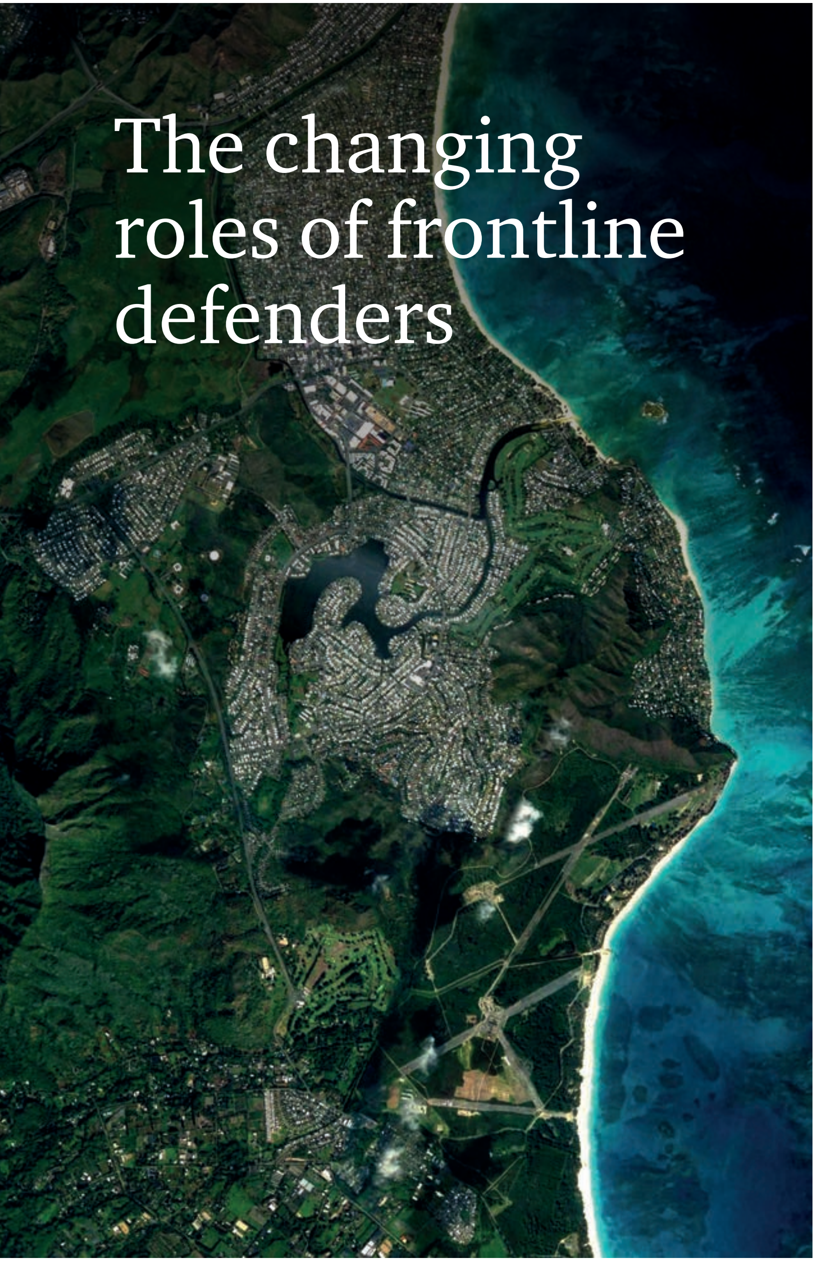
strengths and pain points in the system and can act as a useful framework to show what is working well and where there are weaknesses.

How successful various regions' responses are to COVID-19 will be scrutinised by citizens and academics alike in the coming months and years. Defence and security forces will be tested and used at scale in ways that most civilian populations during peacetime have not experienced. The most recent deployment of defence and security forces for non-military action on a large scale was in response to the 2019 bushfires in Australia and wildfires in California. This deployment also highlighted both the strengths and the weaknesses of public-sector threat responses.

A pandemic is not over in a month or even a year. Institutions will need to continue to respond for the foreseeable future as economies seek to return employees to work, as international travel resumes, and as health services and social care systems reassess their capacities. And as the world reopens, there will need to be a wide-scale operation to monitor infection rates. The SEAM framework provides help in understanding the readiness of the security ecosystem now and in the future.

> Defence and security forces will be tested and used at scale in ways that most civilian populations during peacetime have not experienced.

The changing roles of frontline defenders



Because most defence forces work with an organisational blueprint based on conventional warfare, responding to other kinds of threats requires drastic changes to ways of working. These changes are needed in a pandemic and also when institutions are faced with threats from adversaries that employ hybrid, asymmetrical tactics to destabilise societies and undermine governments. To cover this 'agility gap,' defence forces must be ready to dramatically alter their organisation.

The same is true for the security forces that are now being called on to extend their normal policing duties to enforce emergency measures limiting public gatherings and maintaining public order. Some crimes may be occurring less frequently, but others are increasing during the pandemic. As we noted in our 2018 report, *Policing in a networked world*, crime is moving indoors and online.[1] A pandemic, with its lockdowns and strains on the police, will only exacerbate this trend. Domestic abuse, child abuse and elder abuse may rise unseen. The number of emergency calls for police intervention in homes has already reportedly increased in both the US and the UK.[2] There have been similar warnings about a potential rise in cybercrime and fraud as governments roll out social welfare payments online on a scale not seen before. Cross-border fraud is also an issue as countries scramble to buy medical supplies.[3] In one instance, border control officers in the UK found cocaine hidden in a shipment of medical masks.[4]

The private sector is also part of the emergency response. Supermarkets are trying to manage food and household supply chains as populations panic buy and supplies are limited due to new export regulations.[5] Manufacturers are changing production lines to deliver critical products. Internet providers are having to increase bandwidth because so many people have been forced to work from home. The definition of critical infrastructure is expanding.

[1] PwC, *Policing in a networked world,* 2018: https://www.pwc.com/gx/en/industries/government-public-services/public-sector-research-centre/agile-policing-networks-policing-in-a-networked-world.html.

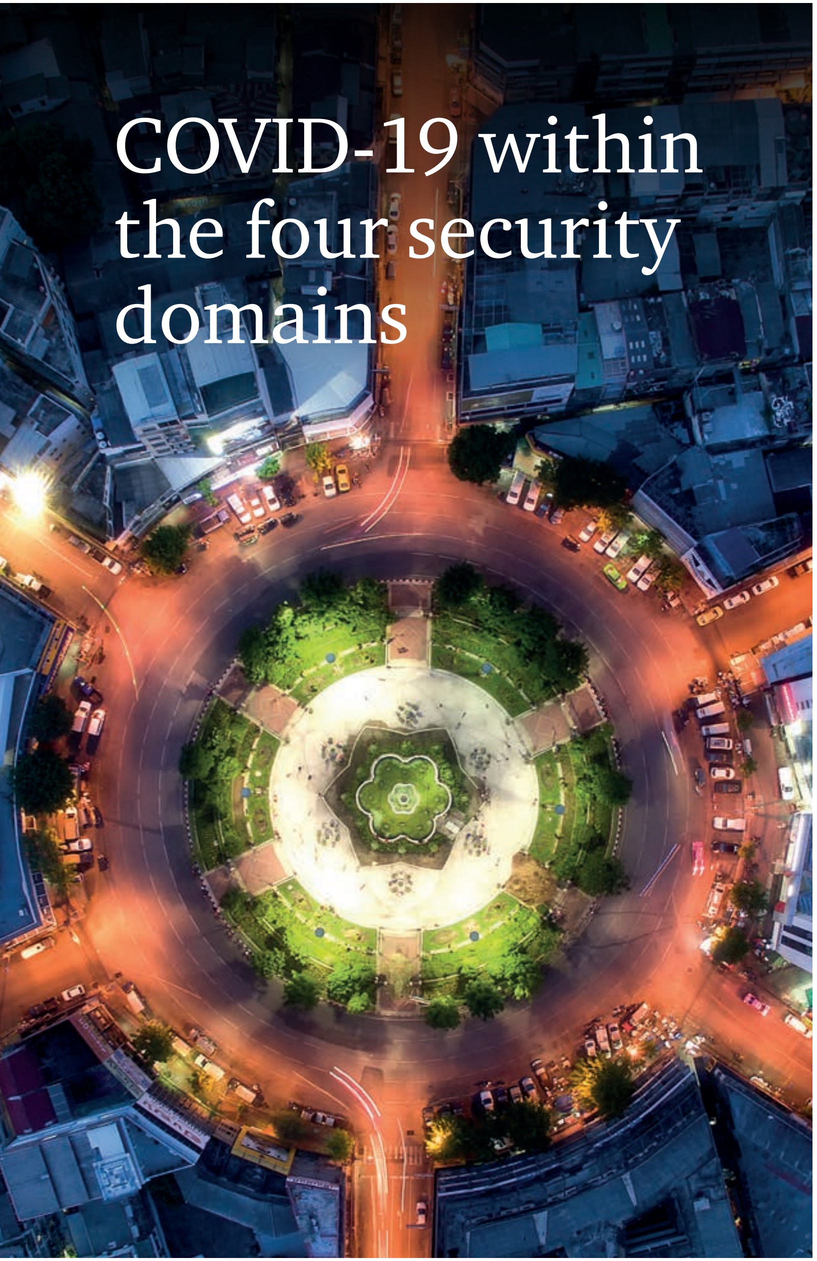
[2] Amanda Taub, "A New Covid-19 Crisis: Domestic Abuse Rises Worldwide," *The New York Times,* 6 April 2020: https://www.nytimes.com/2020/04/06/world/coronavirus-domestic-violence.html.

June Kelly and Tomos Morgan, "Coronavirus: Domestic abuse calls up 25% since lockdown, charity says," *BBC News,* 6 April 2020: https://www.bbc.com/news/uk-52157620.

[3] Interpol, "Unmasked: International COVID-19 fraud exposed," 14 April 2020: https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed.

[4] "Coronavirus: Cocaine haul in boxes of face masks seized," *BBC News,* 15 April 2020: https://www.bbc.com/news/uk-england-52300095.

[5] "The world's food system has so far weathered the challenge of covid-19," *The Economist,* 9 May 2020: https://www.economist.com/briefing/2020/05/09/the-worlds-food-system-has-so-far-weathered-the-challenge-of-covid-19.



COVID-19 within the four security domains

In our 2019 report *Achieving safety and security in an age of disruption and distrust*, we stressed the need for collaboration between the public and private sectors to keep people safe, secure and prosperous.[6] We described how modern threats — terrorism, cyberattacks, food insecurity, climate change, pandemics — are interconnected across four domains of security: economic, social, digital and physical. And we identified steps governments and the private sector can take to mitigate these threats. Trust is at the heart of any response. Emergency measures require populations to believe in and support their leaders. A successful response to a threat, including a pandemic, must be founded on trust.

Unfortunately, trust in institutions and leaders is low. For the past decade, not even half of the people surveyed in the annual Edelman Trust Barometer of ordinary citizens have said they trust their government.[7] But as governments call on their people to take drastic actions in efforts to mitigate disaster, there may be an opportunity for leaders to build back trust.

The various responses around the world to COVID-19 show the stresses put on nation-states by global threats. Many nation-states are turning their attention inwards — shutting borders, shoring up supply chains. News in April 2020 that the US would freeze funding for the World Health Organization came as a shock, especially because institutions will need to work together at the local, national and international levels to battle this pandemic.[8]

There are already examples of sharing medical developments and supplies. In the private sector, global communications companies are working to connect citizens who are separated by circumstances; even video-game companies are being asked to do their bit by embedding 'stay at home' messages in their most popular streaming products.[9] And at the local level, neighbourhoods are working to help the most vulnerable get the support they need even before governments step in. However, such efforts are not yet systemic, and they're not always systematic.

[6] PwC, *Achieving safety and security in an age of disruption and distrust*, 2019: https://www.pwc.com/gx/en/government-public-sector-research/pdf/pwc-achieving-safety-security.pdf.

[7] Edelman, *20 years of trust*, 2020: https://www.edelman.com/20yearsoftrust.

[8] Kai Kupferschmidt and Jon Cohen, "'Short-sighted.' Health experts decry Trump's freeze on U.S. funding for WHO as world fights pandemic," *Science*, 14 April 2020: https://www.sciencemag.org/news/2020/04/trump-freezes-us-funding-who-world-fights-pandemic.

[9] Press Association, "Video games to host Stay At Home, Save Lives message," *The Guardian*, 5 April 2020: https://www.theguardian.com/world/2020/apr/05/video-games-to-host-stay-at-home-save-lives-message.

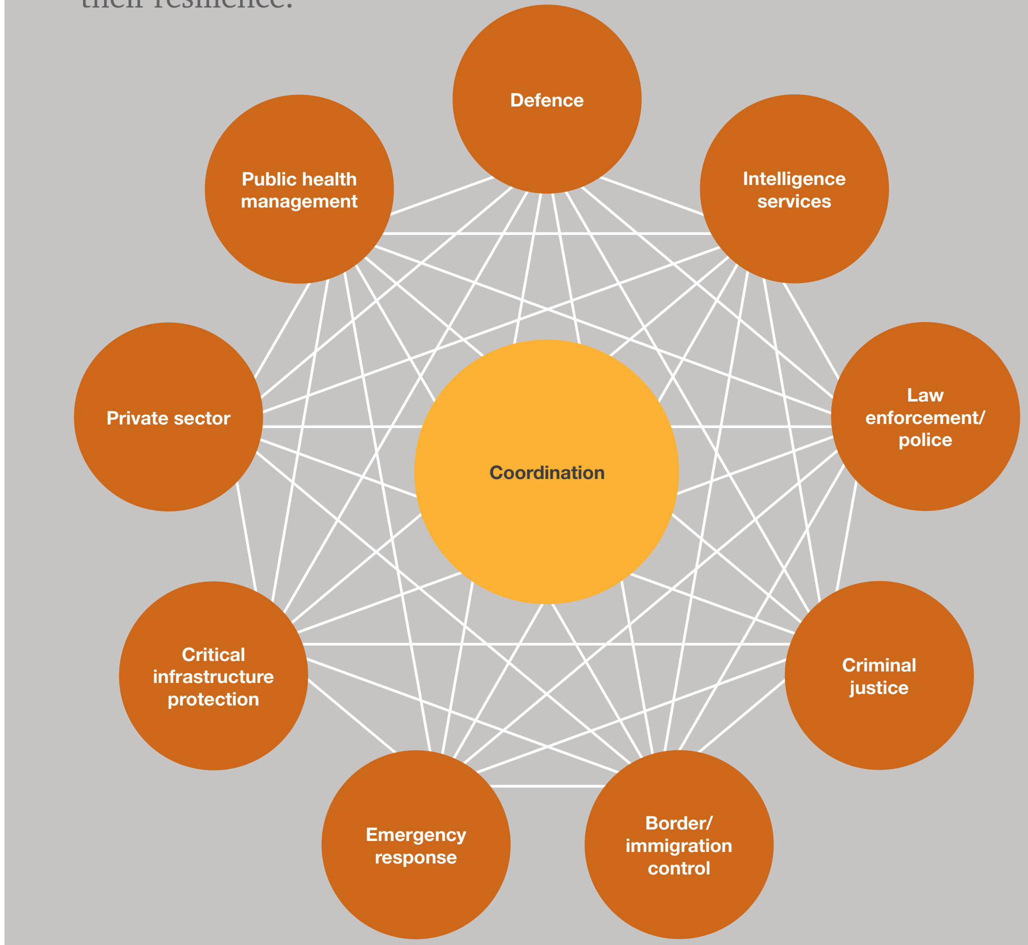
The security ecosystem

If the SEAM framework is applied to the COVID-19 response, it can help identify gaps that can then be addressed to strengthen responses. The SEAM methodology assigns a risk level to the interactions that institutions have with other institutions in the security ecosystem. An appropriate response starts with understanding and identifying the points of connection between the individual entities in each of the relevant national security functions.

When we look at the institutions and actors that have roles to play in keeping citizens safe, we can identify nine key domains that make up the security ecosystem. All or some of these institutions will be involved in the response to a pandemic.

The national security ecosystem

The multiple points of connection within the Security Ecosystem Assessment Map (SEAM) must first be identified and then tested for their resilience.



Let’s look at how the domains interact with one another during a pandemic, where they overlap and what questions leaders should be asking in order to shore up a country’s security system.

In mapping a threat response, the first step is to identify the links that already exist between these institutions and services and assess how robust they are.

In a pandemic, the first domain to be engaged will be public health management — both in the public and private sectors, depending on how citizens access health services. With so many people becoming critically ill so quickly, there needs to be an immediate response to ensure hospitals and staff can cope. Trying to maintain supplies — ventilators and personal protective equipment are top of mind — and free up beds and have enough people in addition to the medical staff to provide services is a logistical challenge. Here, the public health management domain is collaborating with the traditional defence domain, because the military has expertise in all these areas, but that expertise is more typically applied in battlefield conditions. And the private sector is either volunteering or being commandeered to ramp up production of needed supplies. The coordination of these sectors is the responsibility of the government — shown as *coordination* in the model on page 7.

Establishing the process, leadership and points of contact between these various institutions can take time. Defence is usually under federal control; public health may be run at the state or local level. The policies and thresholds for action will vary. Scenario planning in advance can help turn a hypothetical crisis into a successful response. Having hospitals and medical services work with military doctors poses challenges in a non-wartime situation. For example, are triage protocols the same, and if not, how will differences be resolved in a consistent and accountable manner? Will these protocols have to be adapted? Who is in charge of establishing new protocols? These are questions that the leaders of both domains will need to address.

In mapping a threat response, the first step is to identify the links that already exist between institutions and services and assess how robust they are.

At the same time, these domains will be coordinating with emergency responders, including fire services, private ambulances, and even lifeguards in some instances, adding to the complexity and creating a new level of management. And as governments pass laws restricting movement and activities, law enforcement and police forces need to be mobilised to carry them out. This introduces another layer of leadership and management.

The key here is consistency in both advice to the public and application of the law. Thus far, communications in some countries have been inconsistent; police in one region may be handing out fines when those in another region are not. This not only is confusing for people but also affects the trust citizens have in the authorities. And to prevent or stop pandemics in prisons, some governments have also considered releasing prisoners early.[10] Ultimately such an action will involve coordination between the police and the criminal justice system.

Crime often escalates in times of crisis. Cyberattacks, for example, on businesses and government departments have increased as more people have been working remotely, sometimes with lax security protocols.[11] Cybercriminals are also targeting hospitals.[12] Behind the scenes, there will be more pressure on the intelligence services, which will be working with the police and the government.

Then there is the proliferation of misinformation, not only about the causes of the pandemic but about what people should do to prevent it from spreading. Here, social media platforms, built and operated by the private sector, which could be described as critical infrastructure in this crisis, have a role to play both in connecting isolated people and in ensuring that government messages are disseminated and that ‘fake news’ is limited.[13] For example, a number of 5G communications towers in Ireland, the Netherlands and the UK were attacked after videos purporting to link them to the spread of the virus started circulating and, within weeks, had been viewed by nearly 13m people.[14]

This is just one of many threats to critical infrastructure that might arise during a pandemic. Guarding against them requires the interconnection of different domains. There is the telecoms and broadband infrastructure that is supporting the communications for people working from home to help the economy and disseminating public service information. There are the trade policies, the transport infrastructure and logistics systems that governments need to oversee and commandeer to fortify supply chains for critical equipment and food security. The private sector is having to ensure the continued operations of oil refineries and the protection of its staff.

At the very start of the pandemic, many countries were quick to close borders and place restrictions on travel. Border and immigration control must now liaise with several other domains to ensure their protocols take into account health, safety and ethics concerns. In the US, this has become a heated issue, with the American Civil Liberties Union filing a lawsuit calling for the release of detainees who are in high-risk categories for COVID-19.[15]

[10] Francis Pakes, “Coronavirus: Why swathes of prisoners are being released in the world’s most punitive states,” The Conversation, 20 April 2020: https://theconversation.com/coronavirus-why-swathes-of-prisoners-are-being-released-in-the-worlds-most-punitive-states-136563.

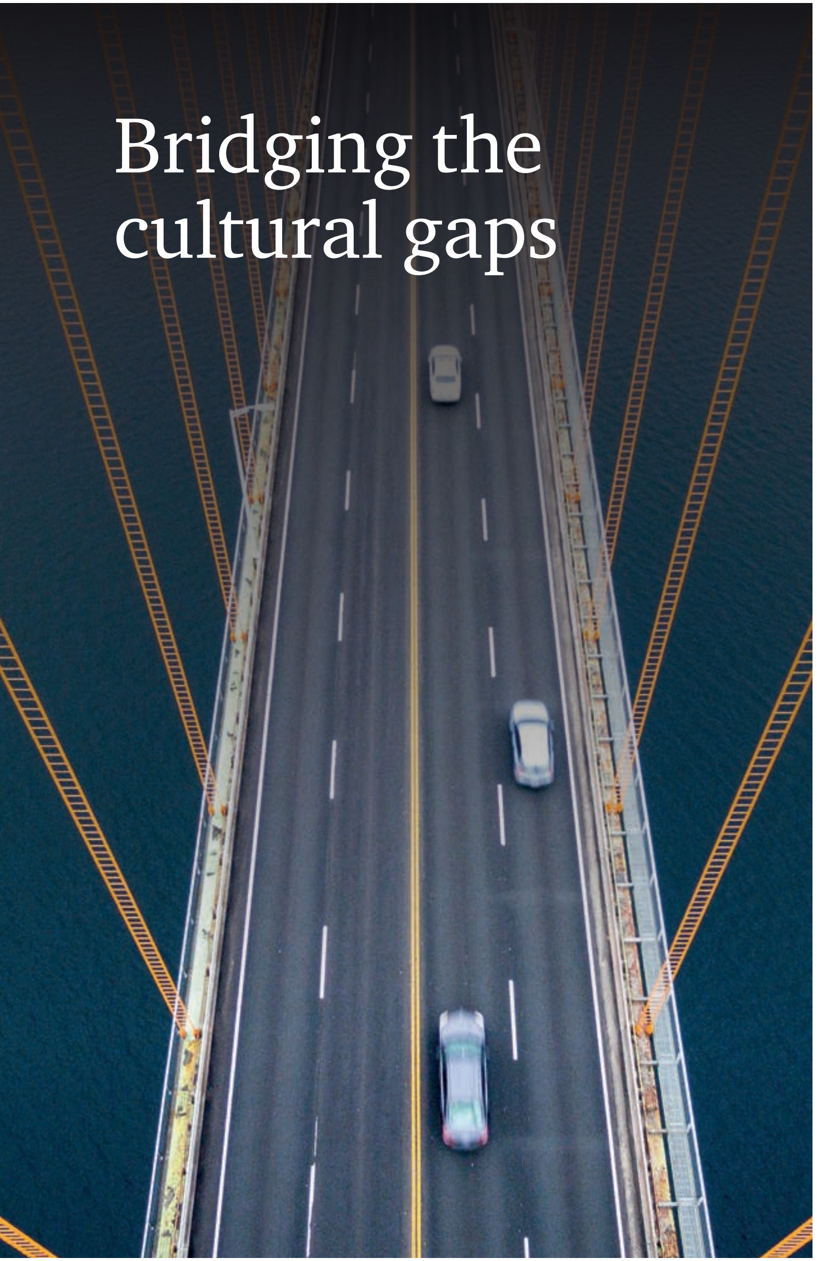
[11] Helen Warrell and Katrina Manson, “State-backed hackers using virus to increase spying, UK and US warn,” *Financial Times,* 8 April 2020: https://www.ft.com/content/37149106-eb16-4b4e-879b-2913b99da84f.

[12] Davey Winder, “Cyber Attacks Against Hospitals Have ‘Significantly Increased’ As Hackers Seek To Maximize Profits,” *Forbes,* 8 April 2020: https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/#3a959e5c58bc.

[13] Julia Carrie Wong, “Coronavirus: Facebook will start warning users who engaged with ‘harmful’ misinformation,” *The Guardian,* 16 April 2020: https://www.theguardian.com/technology/2020/apr/16/coronavirus-facebook-misinformation-warning.

[14] Nic Fildes and Mark Di Stefano, “How a 5G coronavirus conspiracy spread across Europe,” *Financial Times,* 16 April 2020: https://www.ft.com/content/1eeedb71-d9dc-4b13-9b45-fcb7898ae9e1.

[15] Kate Morrissey, “ACLU sues for release of ICE detainees at Otay Mesa Detention Center as COVID-19 cases at facility increase,” *The San Diego Union-Tribune,* 6 April 2020: https://www.sandiegouniontribune.com/news/immigration/story/2020-04-06/aclu-sues-for-release-of-ice-detainees-at-otay-mesa-detention-center-as-covid-19-cases-at-facility-increase.



Bridging the cultural gaps

The cultural differences between institutions and domains that need to work together can also create challenges. This is where leadership is important. In the SEAM framework, cultural differences are bridged at what we call the inter-functional level, where leadership chains of command are established and maintained between the various domains that need to work together in a crisis. Military command is different from civilian command, but in crises the two have to collaborate. For example, army hospitals and civilian hospitals work differently. This can produce a pain point that needs to be acknowledged and addressed. Battlefield priorities in life-and-death situations won’t apply to civilian care.

The above examples of how some institutions and domains will need to work together during the pandemic are not exhaustive. A resilient security ecosystem requires a multitude of public and private entities to interact, interoperate and collaborate domestically and abroad if it is to effectively counter threats and mitigate risks. These entities must do so within the scope of their own function, and also inter-functionally.

In a terrorist threat, for example, organisations with intelligence functions must be able to share information and insights to provide warning or strategic intelligence. Intelligence must meet the information needs of decision makers in other functions, such as defence and government. Inputs to the intelligence picture or actions required to strengthen defences may come from organisations outside the national security domain, such as owners and operators of national critical infrastructure. These critical dependencies must be understood and formalised through governance, regular exchanges and flows of information to achieve security outcomes.

The way forward

This ecosystem itself is not static. Different threats require different entities and functions to coordinate their actions and form strong ‘seams’ where they connect. But policy and cultural barriers and institutional weaknesses introduce vulnerabilities: undefined or confusing accountabilities, poor information flows or blind spots that lead to gaps in a security ecosystem. These weak spots create opportunities for malicious actors to inflict damage on citizens and nation-states. In this pandemic, for example, vulnerable people are being forced to stay at home, many on their own, where they can fall prey to different types of crime, particularly fraud, as mentioned above.

Assessing weaknesses in the relationships between the institutions and organisations that need to work together in a crisis allows governments to make appropriate decisions about where to invest in order to mitigate risk.

COVID-19 is a test of institutional resilience. Understanding where institutions succeed and where they fall short will help everyone better prepare for the next test.

Different threats require different entities and functions to coordinate their actions and form strong ‘seams’ where they connect.

Contacts

Terry Weber
Global Government Defence Network
Partner, PwC Australia
+61 2 6271 3522
terry.weber@pwc.com

George Alders
Global Government Security Network
Director, PwC Netherlands
+31 88 792 3285
george.alders@pwc.com

Catherine Jones
Director, PwC Australia
+61 2 6271 3262
catherine.e.jones@pwc.com

James Coates
Senior Manager, PwC UK
+44 77 1156 2039
james.a.coates@pwc.com

Rianne Siebenga
Manager, PwC Netherlands
+31 88 792 3315
rianne.siebenga@pwc.com

Marketing

Kristin Han
Global Strategic Marketing
+1 347 343 1646
kristin.l.han@pwc.com

pwc.com/SEAM

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 content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.