Crooked States:
How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now

James Cockayne  Head of Office, United Nations University (UNU) Office at the United Nations
Amanda Roth

A Background Study for the UK’s Global Strategic Trends 2050 project, supported by the UK Department for International Development.

This material has been funded by UK aid from the UK government; however, the views expressed do not necessarily reflect the UK government’s official policies.
Table of Contents

4 EXECUTIVE SUMMARY

6 INTRODUCTION: IMAGINING ORGANIZED CRIME AND CORRUPTION IN 2050
   WHAT ARE WE TRYING TO UNDERSTAND?
   Defining organized crime and corruption
   Understanding governance
   Vulnerability, protection and rent extraction
   The importance of policy choices

METHODOLOGY OF ANALYSIS AND STRUCTURE OF THE REPORT

11 1. DEMOGRAPHY, WORK AND MIGRATION
   MIGRATION
   THE FUTURE OF WORK
   GENDER IMBALANCES

14 2. ENVIRONMENT AND RESOURCES
   RESOURCE MAFIAS
   WILDLIFE TRAFFICKING
   FOOD AND ENERGY FRAUD
   CLIMATE VULNERABILITY AND DISASTER

18 3. FRAGILE CITIES AND URBAN GOVERNANCE
   ‘UNPLANNED URBANIZATION’ AND CHALLENGES IN GOVERNANCE
   VIOLENCE AND THE GOVERNANCE OF ILLICIT MARKETS

21 4. VICE MARKETS
   NARCOTICS
   VIRTUAL VICES
   STATES MAKE CRIMES

24 5. CYBERPOWER
   EXPLOITING CYBERVULNERABILITY
   CYBER-PROTECTION
   HACKER CREWS AND CYBERMERCENARIES

27 6. FOLLOW THE MONEY
   ILLICIT FINANCIAL FLOWS
   THE SMART MONEY?
   THE ‘CORRUPTION TRAP’
Table of Contents

33 7. POLICING AND PRIVATE PROTECTION
   A DIVERSIFYING MARKET FOR PROTECTION
   TECHNOLOGY, SURVEILLANCE, AND CYBERPOWER

36 CONCLUSION: STRATEGIC POLICY IMPLICATIONS
   CYBERPOWER AND THE NATION-STATE
   WHAT IS THE ‘PUBLIC INTEREST’ IN A PRIVATELY GOVERNED WORLD?
   INVESTING IN GLOBAL COMMONS AND A RULES-BASED INTERNATIONAL ORDER
   THREE SCENARIOS FOR GOVERNANCE IN 2050
      Hobbes
      Hanseatics of the 21st Century
      Heterogeneity

39 ENDNOTES
Executive Summary

There is a growing recognition that, in many parts of the world, organized crime and corruption reflect larger patterns of wealth-accumulation, power, and governance. Attempting to understand the ways in which organized crime and corruption may change – or remain the same – between now and 2050, then, is an important aspect of understanding the future strategic environment in which states will operate.

How can we hope to understand what organized crime and corruption might look like in 2050? The approach we adopt in this paper is to treat organized crime and corruption as, fundamentally, about the organized extraction of criminal rents. We explore how physical, social, and technological changes will structure the strategic environment in which organized criminal actors, and those that compete with them to control rents – and the resulting governmental power – make their strategic and policy choices. We consider how change will create new opportunities to provide protection, engage in arbitrage, and extract criminal rents – and how these opportunities may create space for criminal actors to exert governmental power.

The central argument throughout this report is that, by 2050, organized criminal groups will use the extraction of criminal rents to play an important role in local, national and, in some areas, global governance. In some cases, they may serve as de facto governmental actors in specific communities, supply-chains, or markets—not only providing protection and services, but also dictating norms and offering meaning and identity to citizens.

We explore how seven different areas of change will create new opportunities – and new constraints – for the extraction of criminal rents: 1) demography, work, and migration; 2) environment and resources; 3) fragile cities and urban governance; 4) vice markets; 5) cyberpower; 6) follow the money; and 7) policing and private protection. Finally, we reflect on the resulting strategic and policy implications for states.

The transformation of work and labour markets as a result of demographic and technological changes will create ongoing migration pressures. Ageing populations will likely create demand for expansion of labour migration, especially in the health, agricultural, and domestic-service industries in the global north. Smuggling markets may become more consolidated and vertically integrated, and the routes, borders, and nodes of human smuggling routes will likely remain key sites of corruption and exploitation. Gender imbalances in some countries may also fuel demand for sex trafficking. Technological changes, including digitization, artificial intelligence, automation and additive manufacturing, will lead to significant disruption in global value chains and resulting job losses in certain sectors and regions, and criminal activity may become a more appealing option for the unemployed.

Changes in the physical environment will also create new opportunities for rent extraction. Mafias and trafficking networks may emerge to govern the distribution and allocation of increasingly scarce resources, including water, food, land, and wildlife products. These groups will serve as brokers in resource-related value chains, matching demand and supply and providing protection (for a price) against uncertainty and risk. An increase in the frequency and severity of extreme weather events may also provide opportunities for criminality and corruption in disaster response and recovery efforts. The opportunities presented by climate vulnerability, however, will depend significantly on how climate change is governed and mitigated around the world.

Fragile cities and unplanned urbanization will be a major site for criminal organization. Fragile cities, especially those affected by natural disasters, will likely be increasingly difficult for local municipal and state authorities to govern. Criminal groups may emerge to provide protection and services to residents in densely populated urban areas not well served by the institutions of the state. They may increasingly offer citizens meaning and identity, and dictate norms around the use of violence. They may also emerge as brokers in informal or parallel economies, and control the gates that connect these spaces and communities to the outside world.

Vice markets — markets for drugs, sex, and gambling, as well as other criminalized leisure and pleasure activities – will likely remain a significant site of rent extraction, but may look very different by 2050. Synthetic drugs may come to dominate the global narcotics market, overtaking marijuana, cocaine, heroin, and other organic narcotics. Additive manufacturing, virtual reality, and a shift to online commerce will change the structure and geography of vice markets – creating new arbitrage and organizational opportunities for criminal groups, and new challenges for law enforcement. But global regulation of vice markets is also likely to evolve, as new vices such as chemically-enhanced virtual-reality emerge, and as some states adapt to take advantage of the opportunities created in these markets, legalizing and taxing certain vices to increase revenue and reduce social externalities.

Cyberpower—the ability to subjugate cyberspace and control digital data—will become an increasingly important source of governmental power. In a world in which the majority of human activity is captured online, the data generated is a highly valuable commodity. This will create new opportunities for rent extraction, and drive new demands for protection. Cyberspace will provide a new venue for competition and collusion between states, criminal groups, and other aspiring governmental actors seeking to provide that protection – and to control the resulting governmental power. Cyberspace will also increasingly provide a new medium and venue for criminal organization, with relatively low barriers to entry and low risk of detection, disruption and punishment. By 2050, cyber-criminality is likely to be highly fluid: governments, businesses, and non-state actors may all see cyber-
crime – and cyberpower – as a way to extend their coercive power and strategic reach.

**Following the money** in 2050 will have elements that seem similar to today – alongside radically different aspects. Illicit financial flows seem likely to remain an important feature of the global political economy; but the vectors and mediums for those flows may change. Virtual currencies and peer-to-peer payment networks may provide significant new and weakly regulated opportunities for non-state (including criminal) organization, and weaken states’ control over revenues, monetary policy instruments, and macroeconomic stability. Illicit financial flows may also be closely tied to high levels of systemic corruption, which may in turn perpetuate inequality and lead to political and social insecurity.

**Policing and protection** will likely also change significantly by 2050, with private actors playing a more overt and significant role in law enforcement and the provision of trust services (from online identity verification to the protection of resource value-chains). Policing functions may shift from public and physical spaces to privately controlled value chains and business processes. Global coordination and partnerships, including with private actors, will be increasingly central to policing these spaces, including cyberspace, financial networks, and global value chains. Technology will present new opportunities for law enforcement, as it will for criminal groups, especially in surveillance and the use of data, but the way that technology is adopted and used will depend on the willingness and capability of individual states – and their policy choices.

**Strategic policy implications**

By 2050, technological, physical and social changes will have generated a variety of new ‘spaces’ and contexts over which states exercise only limited control and governmental power. Criminal and corrupt actors may step into this space – not only providing protection and services, but also dictating norms and offering meaning and identity to citizens. In the final section of the report, we consider different scenarios for how these systems of protection and governance may develop, and the strategic policy implications that follow.

The policy choices states make in the coming years may determine whether organized crime has, by 2050, become fused with the power of states or other governmental actors, or whether it remains largely outside of and marginal to the state and global governance. The risk is that where we see state ‘fragility’ today, by 2050 a highly ‘crooked’ system of governance will have emerged, serving the interests of a corrupt elite – while leaving growing segments of the population vulnerable to environmental, economic, and health insecurity. In this 2050, the lines between public and private blur heavily, and corruption risks becoming the ‘operating system’ of governance in many contexts, particularly those affected by conflict.

Alternately, different actors – including states, municipalities and corporations – may band together to create new, highly secure networks of governance that straddle both physical space and cyberspace. These cooperatives may provide protection and trust services – from secure currency to a secure internet – to their members, while facilitating free trade within and between partners. But individuals and communities operating outside these structures may be excluded from such protection, while political and economic competition may create incentives for collusion with criminal and corrupt actors.

Finally, there is an opportunity for another outcome: one involving heterogeneous but networked global governance, in which private and state actors collaborate to protect public goods, from a democratic and open cyberspace to a protected and secure climate. Securing these common goods, and the rules-based international order, will require investments in protecting these systems – and a changed attitude to organized crime and corruption.

We must recalibrate our responses to organized crime, so that they are not gauged narrowly as technical law enforcement and capacity-building efforts. Instead, they should be understood as strategic interventions designed to undermine the social legitimacy and capital of organized crime, and strengthen the viability, performance and allegiance to state-based, rules-respecting governance solutions.
Introduction: Imagining Organized Crime and Corruption in 2050

Identifying the nature and scope of today’s global organized crime and corruption is a challenging task. Criminal actors are invested in keeping their activities secret, and government sources may also have reasons to distort criminal activity, whether to demonize it or to hide corruption and complicity. Evidence is, in other words, complex. So it may seem like a fool’s errand to attempt to foresee – in even the vaguest outline – what organized crime and corruption will look like in 2050.

Equally, however, there are good reasons to think that an inquiry into the nature and impact of organized crime and corruption is not only useful, but necessary, to understand the patterns of wealth and power – that is to say, of order – that we can anticipate in 2050. There is a growing recognition that, in many parts of the world, if not globally, organized crime and corruption are not marginal to order and governance, but central to it; that there are not two worlds – an upperworld and an underworld, entire and distinct from each other – but one, single strategic space in which state, criminal and other actors compete to govern.2 This recognition lies close to the surface in the 2011 White House Strategy to Combat Transnational Organized Crime, and behind the growing references to organized crime in the discussions and statements of the UN Security Council, as seen in Figure 1 below.

Figure 1. UN Security Council resolutions and presidential statements with references to “organized crime,” 2004-2014

In our effort to understand the future of organized crime and corruption, we seek to identify how an array of physical, technological and social drivers will shape the opportunities and choices for organized crime and corruption, out to 2050. In this paper, we explore how organized crime and corruption may evolve over the next three decades. In particular, we were asked to look at how the changing nature of organized crime and corruption may relate to state fragility, inequality and conflict.

In this paper, we engage in a foresight process, intended to imagine and sketch the direction of travel in the evolution of organized crime and corruption, out to 2050. This is not a forecast, nor a prediction. As we make clear in more detail below, we believe that the outcomes in 2050 depend significantly on strategic policy choices made by governments in coming years – but also the choices made by criminal actors themselves. Outcomes are not structurally predetermined; strategic actors (including those with criminal and even kleptocratic agendas) react to parameters set by their strategic environment. Thus, an understanding of how the strategic environment is likely to change out to 2050 – as a result of physical, technological and social drivers – can help us understand what choices those actors have to make. It can help us understand the menu of options from which criminal actors will be choosing, and the impacts their choices will have. And it can help us think about the import of states’ and international organizations’ policy choices in the near and medium term, to understand what directions they may take us in.

In this paper, we seek to identify how an array of physical, technological and social drivers will shape the opportunities and choices for organized crime and corruption, out to 2050. This section defines what we mean by ‘organized crime’ and ‘corruption’, and situates those terms against the notions of ‘protection’ and ‘governance’; explains our analytical methodology; and details the structure of this report.

What are we trying to understand?

Defining organized crime and corruption

‘Organized crime’ and ‘corruption’ are both highly contested terms, used to refer to widely varying phenomena.3 For example, the term ‘organized crime’ is sometimes used to refer to the ‘who’ – the organizations behind organized crime – and at others to the ‘what’ – the criminal activities themselves.4 The definition of corruption, similarly, varies across legal and cultural contexts.5 And both the popular and academic consensus on what constitutes organized crime and corruption change over time: what we understand as corruption may look very different in thirty years than it does today.6

In our effort to understand the future of organized crime and corruption, we attempt in this report to focus on the con-
Economic rents are frequently associated with organized crime, corruption and governance. We treat organized crime and corruption as distinct but related phenomena, both concerned with the extraction of criminal rents.

Our object of inquiry

A ‘criminal rent’ is the value beyond the costs of production that is extracted either a) from the supply of a criminalized good (such as cocaine) or a criminalized service (such as illegal prostitution), or b) from the supply of a legal good or service, but in a criminalized manner (such as black market sales).

Economic rents may be considered a measure of ‘market power’ – the ability of one buyer or seller in a market to ‘exert significant influence over the quantity of goods and services traded or the price at which they were sold’. Such rents are often created by scarcity, either due to limited supply, as in the case of resources such as land, or artificially created scarcity, as in the case of government licensing or monopoly control. Criminalization is, itself, a form of licensing. By criminalizing the supply of a specific good or behaviour, states create the opportunity for the extraction of criminal rents, by circumvention or non-enforcement of criminal norms.

Organized crime involves the development and maintenance of organizations that extract such rents. Corruption involves the abuse of a public position of trust for private gain – and is frequently aimed at the extraction of criminal rents. ‘Petty’ corruption involves lower-level office-holders; ‘grand’ corruption typically involves political and senior public office holders. When considering corruption, this paper focuses in particular on the latter, grand corruption – the organized or systematic exercise of official governmental authority for illicit gain.

The motivations for participation in organized crime or corruption are, of course, multiple. While participants are frequently driven by pecuniary considerations, they may also be driven by a desire for power or honour, or by fear. But understanding how broader systems of criminal power and control function generally requires understanding the resource flows, and associated rents, that underpin those systems. Focusing our inquiry on where and how criminal rents will be extracted, therefore, allows us to think more systematically about how crime and corruption may be organized in 2050 – by thinking through where rents may arise or be extracted in 2050, how their extraction will be protected and governed, and how that differs from (and remains similar to) today’s patterns. Understanding where and how criminal rents will be extracted is critical to understanding where crime and corruption will become organized, and the strategic environment in which they operate.

Economic rents are frequently associated with rent-seeking, or the practice of ‘manipulating public policy or economic conditions as a strategy for increasing profits’. Not all criminal behaviour is rent-seeking; in some cases, criminal groups simply operate in an existing market, subverting but not seeking to alter the norms that govern that market. But in other cases, organized criminal groups may seek to govern these markets, changing the strategic environment in which they operate to maximize opportunities for rent-extraction. That often involves corruption of public authorities and institutions, and it is those cases that have particular implications for the future of governance – both licit and illicit governance – and the interaction between criminal groups and the state.

Understanding governance

Our inquiry requires careful reflection on the physical, social, and technological changes that will shape the world in the coming decades, including demographic changes, such as ageing populations, urbanization, and changes in global economics and inequality; environmental changes, such as climate change and resource scarcity; and technological changes, such as digitization, automation, changing supply chains, and the evolving nature of currency and finance. Each of these shifts will lead to new opportunities – and new constraints – that will dictate where criminal rents may be extracted, and how different state and non-state actors will adopt different strategies for exploiting these opportunities.

Although ‘organized crime’ and ‘corruption’ are the objects of our inquiry, the story we tell is thus centrally one about how society is ordered and regulated, which is to say, its governance: how norms are developed and enforced, and resources accordingly allocated. Understanding how and where rents may be extracted allows us to better focus on the strategic impact of crime and corruption, and provides a window into the role these forces will play in governance – especially informal, illicit, or invisible governance – in the decades to come.

The relationships between organized criminal groups, states and societies in 2050 will, however, vary in different places. In some cases, states and criminal organizations may cooperate, or even collaborate, to maximize their governmental power, while in other cases they will compete for that power. And in some cases, the personnel involved in running the state and organizing crime may become intimately entwined, into what Sarah Chayes describes as ‘transnational kleptocratic networks’. The forms these relationships may take, and the way in which the nature of organized crime and corruption may change by 2050, are discussed in more detail in the concluding section of this report.
The organized extraction of rents at sites of arbitrage often requires protection – from the interference of the state, or other actors seeking to control and govern – if it is to be sustained. As Frederick Lane made clear in his masterful analysis of corruption and tribute in the Venetian Republic, that protection is often likely to be purchased from other governmental actors, if the cost of purchasing such protection is lower than the resulting net benefit over time.\textsuperscript{17} But protection can also be supplied from within the enterprise, rather than purchased from another, and even sold on to others – not just at these ‘gates’ or points of arbitrage, but wherever else they suffer vulnerabilities and require protection\textsuperscript{18}.

As we illustrate throughout the report, criminal groups will, in many cases, be well-positioned to exploit the opportunities created by these vulnerabilities – and to extract criminal rents. But different criminal actors will exploit such opportunities in different ways. One line of argument, for example, suggests that there are two types of actors: the ‘criminal entrepreneurs’, or those who supply and move illicit goods in criminal markets, and ‘protectors’ or ‘violent entrepreneurs’, who supply protection in these markets.\textsuperscript{19} These two categories of actors represent ideal types; in reality, members of the same criminal enterprise may play both functions.\textsuperscript{20}

In this report, we focus in particular on how some criminal actors use the market power they develop – including through supplying protection – to govern those markets, setting and enforcing norms, allocating resources, and resolving disputes. Understanding criminal governance – how and where it may emerge, and what forms it may take – is critical to understanding the impact that organized crime and corruption will have on the larger strategic environment in which they operate. We attempt to identify how and where vulnerability may emerge by 2050, how these vulnerabilities will create new opportunities for illicit activity and protection, how that protection may lead to criminalized or ‘crooked’ governance – and what implications this may have for broader patterns of governance.

\textbf{The importance of vulnerabilities}

Understanding how organized crime and corruption may work in 2050 requires an inquiry into how social, technological and physical changes will generate vulnerability and, in turn, drive new demands for – and suppliers of – protection, from the effects of climate change and economic and political life will be governed not by states but by ‘crooked’ actors, using public forms and institutions to serve private interests, even as they meet the protection and service provision needs of populations and markets.

\textbf{Our argument}

We argue that by 2050, some organized crime groups will use the extraction of criminal rents to play an important role in local, national and, in some areas, global governance. In some cases, they will serve as de facto governmental actors in specific neighbourhoods, supply-chains, markets, or communities. They may not only be providers of services, and physical protection, but also of social protection and systems of meaning and identity, competing with states to supply norms and structure to consumers and citizens. In other cases, organized crime networks will be threaded through elites, and the institutions of states and global governance, penetrating through the loopholes offered by corruption.

As a result, fragile states – and indeed some aspects of global governance – will not so much ‘fail’ in the face of stressors such as climate change, artificial intelligence and additive manufacturing – as become ‘crooked’. Systems of public governance will be corrupted and twisted away from their proper purpose. Sovereignty and the rule of law may be corrupted by private and often criminal interests, and some areas of social, economic and political life will be governed not by states but by ‘crooked’ actors, using public forms and institutions to serve private interests, even as they meet the protection and service provision needs of populations and markets.

\textbf{Vulnerability, protection and rent extraction}

Both organized crime and corruption are inherently opportunistic ventures. Individuals and groups generate and exploit opportunities in their environments to extract criminal rents. Those opportunities frequently arise at the points of arbitrage, the ‘gates’ between realms, markets or communities governed by different actors: at border crossings; at the boundaries between different markets or jurisdictions, where smuggling networks can benefit from price arbitrage; at the legal and financial boundaries between different tax and regulatory jurisdictions; at the boundary between the legal and the illegal.\textsuperscript{16} A rent is extracted in return for safe passage through the gate, across the boundary, from one sphere to another.

The organized extraction of rents at sites of arbitrage often requires protection – from the interference of the state, or other actors seeking to control and govern – if it is to be sustained. As Frederick Lane made clear in his masterful analysis of corruption and tribute in the Venetian Republic, that protection is often likely to be purchased from other governmental actors, if the cost of purchasing such protection is lower than the resulting net benefit over time.\textsuperscript{17} But protection can also be supplied from within the enterprise, rather than purchased from another, and even sold on to others – not just at these ‘gates’ or points of arbitrage, but wherever else they suffer vulnerabilities and require protection\textsuperscript{18}.

As we illustrate throughout the report, criminal groups will, in many cases, be well-positioned to exploit the opportunities created by these vulnerabilities – and to extract criminal rents. But different criminal actors will exploit such opportunities in different ways. One line of argument, for example, suggests that there are two types of actors: the ‘criminal entrepreneurs’, or those who supply and move illicit goods in criminal markets, and ‘protectors’ or ‘violent entrepreneurs’, who supply protection in these markets.\textsuperscript{19} These two categories of actors represent ideal types; in reality, members of the same criminal enterprise may play both functions.\textsuperscript{20}
criminal prohibitions. This definition changes over time and across contexts. Activities that are today labelled and defined as organized crime activities – such as the production and distribution of marijuana – may, by 2050, be normalized and legalized, while activities that are not, today, considered criminal – such as the use of offshore tax havens – may be considered as such thirty years from now. Policy choices that states make now will shape the opportunities for organized crime and corruption in the years ahead.

How policy will shape the result
Identifying the sites of criminal rent extraction is fundamentally about identifying opportunities for arbitrage, protection and circumvention of lawful governmental authority. But the site and nature of the gates between ‘realms’ where arbitrage occurs, and where vulnerabilities emerge that give rise to protection needs are, in turn, products of policy choices by states – and of choices by other actors to develop and shape realms below, outside or beyond the governmental power of the state.

But not only states’ choices. Criminal actors also make strategic choices. Criminal groups do not simply respond to drivers in the environments in which they operate; instead, they adapt to exploit the opportunities and evade the restraints in those environments, including by penetrating, corrupting and bending states and their policies. Any predictions about the future role of organized crime must also predict the constraints imposed by state actors – and the way in which criminal groups and states interact, compete, and collude with each other. 21

Methodology of analysis and structure of the report
Our research and analytical process for this report comprised five steps.

First, we conducted a literature review of the major physical, social, and technological changes expected globally by 2050, with a view to understanding where criminal rent extraction may occur in 2050. We looked for both consensus and disagreement on global megatrends and anticipated changes, including:

- demographic and economic factors, such as population and ageing, urbanization, health, and inequality;
- environmental and physical factors, such as climate change and resource scarcity; and
- technological trends, such as digitization, automation, manufacturing and global supply chains, and digital economy and currency.

Conducting a full literature review on each of these topics individually was, due to time and capacity constraints, beyond the limits of this report. Instead, we focused on reviewing the literature on global megatrends, identifying key areas of consensus and disagreement in our review, and concentrating on areas of relative accord. We were also forced, by necessity, to make editorial decisions about which trends should and should not be included, and to guess at which trends may have the most significant implications for the future of organized crime and corruption.

Some future trends are easier to predict than others. Empirically robust data on population and urbanization projections, for example, is readily available from the UN Department of Economic and Social Affairs. Technological trends, on the other hand, are much more difficult to predict, and there is often little consensus on where and how technological developments will occur. It is increasingly accepted, for instance, that developments in machine learning, automation, and robotics will significantly disrupt the current economic landscape. But there is little agreement on the way that artificial intelligence will develop, the forms it may take, and how it may be adapted by different societies. In the final report, therefore, we chose to focus primarily on the larger socio-economic shifts that would result from automation or other megatrends, and avoided delving into the multitude of possible forms that developments may assume. Nor did we aspire to predict major geopolitical events in the coming decades.

Where possible, we prioritized available data sources, literature, and journal articles with a global scope, especially literature from international organizations such as the United Nations. Where relevant, we supplemented this review with additional research into specific trends. In general, we prioritized research and data from 2010 or later.

Second, we conducted a literature review focused on trends in organized crime, corruption and law enforcement. We focused on what is known and unknown about patterns in each of these areas, and how they may evolve in the future. Key themes that emerged related to:

- the impact of globalization on the relationship between organized criminal groups, corruption, and the state;
- the changing relationship between organized crime, violence, and armed conflict; and
- trends in the structure and operations of organized criminal groups.

Third, and closely related, we conducted a review of available data sources, grey literature, and journal articles to understand the trends in today’s most prominent criminal markets, and in emergent criminal markets. Data on organized crime is notoriously difficult to reliably collect, and trends are consequently difficult to assess. Measurement of criminal activity generally relies on proxy measures, such as volumes of drugs seized, illicit financial flows identified, and, especially in the case of corruption, public perception surveys. Notwithstanding the limitations of available data, we reviewed trends in violent crime and homicide, drug trafficking, arms traffick-
ing, forced labour, human trafficking and smuggling, wildlife and resource trafficking, counterfeiting and pirated goods, cybercrime, and other criminal markets. We also conducted an overview of trends in corruption and governance, and reviewed available data on illicit financial flows and corruption. Again, we prioritized data supplied by international organizations, with a multi-country or global scope, and focused our research primarily on data and literature published since 2010.

Fourth, drawing on these internal, unpublished literature reviews, we identified a set of key ‘drivers of change’ that may shape the future of organized crime and corruption, and drew some initial findings on how they may impact organized crime and corruption out to 2050. These initial findings were tested in a small expert workshop, held in New York, that brought together experts on organized crime and corruption from academia, international organizations, government, think tanks, and nongovernmental organizations.

Predicting future outcomes based on current trends and projections is an inherently flawed exercise. To identify key drivers and possible future trajectories, we focused on the larger physical, social and technological changes where there was relative expert consensus – for example, the ways in which the environment may change by 2050 – and where such shifts may create vulnerability or possibilities for the extraction of criminal rents. We then drew upon current trends in organized crime and corruption to help us imagine how criminal and corrupt actors might exploit the opportunities presented by these shifts, and how states might respond.

Fifth, and finally, the final results of our inquiry are presented in this report. The report is structured to discuss how organized crime and corruption is likely to work in seven broad areas:

1. Demography, work and migration
2. Environment and resources
3. Fragile cities and urban governance
4. Vice markets
5. Cyberpower
6. Follow the money
7. Policing and private protection

A draft of this report was presented at a workshop in London in June 2017, which brought together experts on organized crime, corruption and governance from across government, non-governmental organizations, and academia. In addition to this report, we also produced a policy brief, entitled ‘Preventing the Rise of Crooked States’, that explores the near-term policy implications of the conclusions reached in this report, and what they may mean for development and stabilization efforts. This brief is available online as a separate document.

These results are not intended to be predictive: rather, they are intended to offer a diversity of possible outcomes, and to help policy-makers understand how actions taken in the near-term may impact long-term consequences. We do not expect that all outcomes outlined in this report will come to pass, nor that all criminal actors will behave in the same way. Rather, these developments will likely occur differently in different regions, and at different paces – while some may not occur at all. New avenues for future organized crime and corruption, resulting from trends not discussed here (or not yet imagined), will also arise. (In a summary box for each section, we also note ‘gamechangers’ that could radically change the outlook in each area.) And of course, as is discussed throughout the report, the policy choices that states make in the coming years – in areas as diverse as cyber policy, environmental policy, and migration policy – will profoundly shape both the opportunities and constraints that will dictate the environment in which organized crime and corruption will operate. The final section of the report considers what these changes mean for broader patterns of governance, and resulting strategic policy implications.
1. Demography, work and migration

**Significant dynamics to 2050:** The market for the irregular movement of people will likely persist in the coming decades, with large-scale migration flows from the global South to Europe, North America, and East Asia. Organized criminal groups will likely play an even larger role as the current market, which is highly fragmented, matures. Migration-related locations, such as routes, borders, and detention centers, will remain key sites of corruption and rent-extraction.

**New protection challenges:** Technological changes, including digitization, artificial intelligence, automation and additive manufacturing, may lead to significant disruption in global value chains and result in job losses in certain sectors and regions. In those states that are unwilling or unable to provide broad-based income support, large numbers of people may be left searching for survival, coping and livelihood strategies – making criminal activity a more appealing alternative. Gender disparities in some countries may also create demand for sex trafficking and sexual exploitation.

**Key implications for governance:** The opportunities for criminal rent extraction in the migration market will depend on how states react to and govern migration flows. Some states may invest in safe and orderly migration, while others may harden their borders and increase enforcement. The ‘gates’ between unsafe, irregular migration routes, and regular, safe migration routes, will be key sites of rent extraction. The social and labour market policy choices made by states will also determine available economic opportunities, social protection arrangements, and the resulting demand for irregular migration.

**Potential game changers:** Significant changes to border policy and enforcement; economic or geopolitical shifts that alter migration paths; major, multi-country natural disaster or conflict that affects migration flows; widespread adoption of universal basic income or other expansions of social protection models.

Between now and 2050, the world’s population will continue to grow, although more slowly than in the recent past. By 2050, the UN estimates, the world population will increase to 9.7 billion people. But its centre of gravity will shift: the greatest population growth will occur in lower-income countries in Africa and Asia, while in high-income countries in Europe, Asia, and North America, birth rates will decline and populations will age. Labour markets will also morph, as automation leads to declining jobs in manufacturing and some other low-skill sectors, while ageing populations in Europe and elsewhere create additional demand in the health care industry or other sectors. And today’s gender-selective behaviours in some states – sex-selective abortion or female infanticide, for example – will lead to later gender imbalances in countries such as China and India. The resulting changes and patterns will offer significant opportunities for organized criminal rent extraction and corruption.

**Migration**

Disparities in demand for labour of all kinds will create ongoing migration pressures. Where imbalances between labour demand and supply persist, the resulting flows of people into illegal jobs, or into legal jobs but moving illegally, will create opportunities for organized extraction of criminal rents through human smuggling (and trafficking), and for corruption. The way in which the market evolves through 2050 will depend significantly on state policy choices, and the pattern and flow of migrants and associated criminal rents will shift as legal norms and policy evolve.

Ageing populations in Europe, East Asia, North America and the Gulf countries, combined with youth bulges in some countries in sub-Saharan Africa and South Asia, will continue to drive significant migration flows through 2050 – presenting significant opportunities for criminal rent extraction. Populations are expected to age in most parts of the world, as demonstrated in Figure 2 (overleaf), but this trend will be most pronounced in Europe. A number of historically fragile countries in Africa and Asia, such as Somalia, Afghanistan, Pakistan, and Yemen, will continue to experience significant population growth, creating additional demand for migration.

“The impact and scale of the criminal rents to be extracted from global migration flows will depend on how states react and govern these flows.”
will maintain chronically young populations. Today’s drivers of migration, including conflict, state collapse, poverty, and state repression, will likely continue to power global migration flows, while the effects of climate change, such as extreme weather events, resource scarcity, and environmental degradation, may amplify displacement, and add to the vulnerabilities of those displaced.

The impact and scale of the criminal rents to be extracted from global migration flows will depend on how states react and govern these flows. Traditional destination countries in Europe, North America, and the Gulf may harden their borders and devote law enforcement resources to policing against irregular migration. Yet the latest evidence suggests that these human mobility markets are highly price-responsive. Organized criminal groups and corrupt actors can be expected to take advantage of the ‘criminal tariff’ they can charge for circumventing hardened border controls. Policies intended to harden borders may risk increasing the opportunity for rent extraction and corruption. On the US-Mexico border, for example, smugglers appear to command higher prices when enforcement efforts increase.

**Figure 2.** Percentage of the population over the age of 65, 2015–2050


Over time, the informal market for movement of people, which is currently highly fragmented, is likely to ‘mature’, or become more consolidated and vertically integrated. That will also probably lead to greater involvement of other, professionalized, organized crime groups – as we already see in Central America – and a closer integration between illicit mobility services and illicit labour exploitation – as we are already seeing in Libya, which is increasingly recognized as the site of major slave-trading markets.

Migration-related locations, including people-smuggling routes, borders, and detention centres, are likely to remain key sites of corruption, exploitation, and organized crime. Already, in southern Italy, the mafia reportedly makes more from exploiting refugees and migrants than from the drug trade. However, it is also possible that wealthy countries, faced with a decline in working-age populations, will invest in the development of safe, regular and orderly migration to bolster shrinking workforces and mitigate the risks from chronic, large-scale, irregular migration. Even then, smugglers and traffickers will continue to take advantage of countries with more porous borders, including where officials are more vulnerable to corruption. States’ regulatory policy choices, and the resulting regulatory geography, will determine where the ‘gates’ between irregular and unsafe, and more regular and safe, migration routes and processes are situated. That, in turn, will determine the sites of criminal rent extraction.

**The future of work**

The patterns of human mobility will also be significantly affected, however, by the changing nature of work. By 2050, technological advancements and developments in machine learning, artificial intelligence, digitization and additive manufacturing may lead to job loss across a wide range of sectors, significantly disrupting labour markets. This may increase opportunities for criminal exploitation, but also presents opportunities for innovation and adaptation by states.

While it is largely agreed that automation leads to the decline of employment in routine-intensive occupations, such as manufacturing, office and administrative support, and sales, recent evidence shows that even more significant swaths of the labour market may be vulnerable to automation, including the transportation, education, and healthcare sectors. In the United States, for example, as much as 47 per cent of total employment may be at high risk of automation in the next two decades; this includes a substantial share of employment in the service industry, where most U.S. job growth has occurred in the past few decades. In Japan, up to 55 per cent of current jobs may be vulnerable to automation (although the actual effect on unemployment numbers may be mitigated by population decline). In addition, job losses may extend beyond the industries directly affected by automation. Acemoglu and Restrepo found that, of U.S. job losses caused by the proliferation of industrial robots between 1990 and 2007, only 50 per cent resulted from robots directly replacing workers; the other half of resultant job losses arose in surrounding communities where factories or industries had shut down. They also noted that communities where jobs were lost due to the effects of automation were slow to recover.

Manufacturing jobs are particularly vulnerable to automation: Boston Consulting Group estimates that ‘the share of tasks performed by robots will rise from a global average of around 10 percent [in 2015] to about 25 percent across all manufacturing industries [in 2025]. The advent of additive manufacturing will likely further disrupt the organizational and economic landscape of manufacturing – and global supply chains. Parts may no longer need to be sourced from many different countries and transported over long distances; instead, a design for a new product needed in a specific location could
“Technological disruptions to global value-chains may significantly alter economic geography. Those states that are unable or unwilling to provide broad-based income support may face large numbers of people searching for survival, coping and livelihood strategies. Criminal livelihoods may become more thinkable.”

be emailed to a 3D printer and produced nearby, from start to finish. Related low-skilled jobs, such as assembly, packaging, and shipping, may decline, while the demand for designers and engineers, may increase. These changes in the technological base of manufacturing and distribution are likely to significantly disrupt some global value-chains, possibly allowing global corporations to move from globally distributed production chains to local additive manufacturing centres serviced by automated distribution fleets. Economic geography, especially of manufacturing, may change significantly.

How automation and technological advances will affect the future of work, is, however, harder to predict. The loss of jobs in some sectors may lead to the creation of entirely new human-staffed jobs in those sectors, or elsewhere. Employment may be more heavily concentrated in sectors that require high levels of creativity or particular types of human interaction.

And the social and labour market policy choices states make to help workers displaced from low-skill manufacturing and service-sector jobs into new roles will be highly determinative of outcomes. States may take a more active role developing new labour markets; in China, for example, where local manufacturers are increasingly buying internationally produced industrial robots, the government is investing in the domestic robot industry.

Wealthier states may even begin to reconsider the expectation of pervasive (if not universal) employment, moving instead to provide broad income support, recasting the role of ‘work’ in our lives altogether.

But different states will adapt differently, and some states, especially those faced with rapid population increases, may be poorly equipped to respond to these broader economic shifts. In those states that are unable or unwilling to provide broad-based income support, and do not receive external assistance (for example from multilateral banks) to do so, these disruptions could leave large numbers of people – especially young people – searching for livelihoods and coping and survival strategies. Criminal livelihoods may become a more thinkable alternative – or, in some places, unavoidable.

Gender imbalances

Women and girls are likely to be particularly vulnerable to the harms that result from reduced barriers to criminal work. This may be particularly exacerbated by the emergence and persistence of significant gender imbalances in some countries and regions, driving trafficking for sexual exploitation – the victims of which are already thought to be 96 per cent female.

Sex-selective abortion, female infanticide, and female selective neglect have led to disproportionate sex ratios in a number of countries, including Albania, China, India, and South Korea. Such imbalances take decades to correct; in China and India, for example, men will likely outnumber women by significant ratios in 2050, as illustrated by Figure 3 below.

Figure 3. Number of men expected to want to marry per 100 women expected to want to marry, forecast

This gender imbalance may lead to high levels of human trafficking and sexual exploitation of women and girls from other countries. Using the internet to facilitate operations, organized criminal groups will likely be able to recruit, control, and exploit trafficking victims on a larger scale, managing dozens of victims at once.

Source: “Bare Branches, Redundant Males,” The Economist, 18 April 2015.
2. Environment and resources

**Significant dynamics to 2050:** Organized criminal groups will likely be increasingly involved in the control and distribution of everyday resources, including water, food, and land. In some regions, ‘resource mafias’ or trafficking networks may emerge to govern the distribution and allocation of increasingly scarce resources. An increase in the frequency and intensity of extreme weather events due to climate change may also create new vulnerabilities and provide a range of opportunities for criminal rent extraction.

**New protection challenges:** Water and food scarcity may lead to resource insecurity, creating demand for protection against uncertainty and risk. Criminal involvement in resource supply and distribution may create significant negative externalities, such as price-gouging, contaminated resource supplies, and circumvention of environmental standards. ‘Food fraud’ may also proliferate, leading to significant market segmentation: wealthy consumers may be increasingly willing to pay a premium for brands reputed to have higher supply-chain integrity, while low income consumers will be vulnerable to health and safety risks. Vulnerability to natural disasters and rising sea levels may also create new demands for protection and challenge state institutions.

**Key implications for governance:** Environmental and resource governance will likely be highly contested, and the rewards of circumventing or cheating environmental protections or resource-sharing arrangements will grow. Criminal groups may collude with governments or private companies to penetrate resource-related supply chains, leading to ‘crooked’ environmental governance. Resource mismanagement or scarcity may also increase the potential for conflict, creating spiralling governance challenges.

**Potential game changers:** Significant international agreement(s) to reduce impact of climate change; technological breakthroughs mitigating resource scarcity (i.e. meal-replacement products); major catastrophic weather event that significantly impacts large swaths of the global economy.
control of resource-related value chains, particularly when those chains are highly disarticulated and risks are driven down to those at the bottom. The Sicilian mafia, for example, emerged as violent brokers (and protection providers) within the supply-chains connecting Sicilian hinterland producers of citrus, wheat and rubber with coastal elites and northern Italian capital. Likewise, the New York Mob rose to wealth and power by controlling not only the supply of (illegal) liquor, during Prohibition, but also the supply of poultry, milk, and other foodstuffs.

But they also extract significant rents in return, and create significant externalities, borne by the public – from price-gouging to circumvention of environmental standards. Years of illicit toxic waste dumping in southern Italy, for example, have caused severe environmental degradation, damaged local agricultural markets, and led to abnormally high cancer rates for residents. And in Central America, drug trafficking organizations have contributed to deforestation by purchasing and clearing forested land, which is used to launder narcotics profits, build clandestine roads and landing strips for drug profits, and monopolize control of contested territory.

Criminal actors will likely seek to exploit the opportunities created by resource scarcity and environmental and climate disruption. They may penetrate supply chains for high-demand or highly regulated goods, provide protection against uncertainty and risk, and cooperate or collude with governments or private companies to exploit these markets. Resource value chains will likely attract a variety of armed political, criminal and social entrepreneurs seeking to develop governmental power. In eastern Democratic Republic of Congo, for example, both armed groups and factions of the military have become increasingly involved in the transnational trafficking of gold, diamonds, timber, and other resources. Although political grievances still play a role in the conflict, much of the current violence and instability has been attributed to these activities. Mexican cartels, similarly, are reportedly involved in the supply chains that transport avocados, limes, and other agricultural products to the United States. And as pressure from counter-narcotics efforts led to a decline in drug-trafficking profits in Latin America, criminal groups moved into the illicit gold trade. In Peru and Colombia, the value of illicit gold exports has exceeded the value of cocaine exports.

Water scarcity is likely to be a particular driver of corruption and criminal rent-extraction. By 2040, more than 50 per cent of the world’s population may live in water-stressed areas, as demonstrated in the map below. Of these, over 30 countries will experience extreme water stress, with more than half of them located in the Middle East. In many regions, corruption, embezzlement, and crime have been linked to high levels of waste and increased spending in the water sector. Already, in New Delhi and Karachi, where corruption, pollution, and poor infrastructure have exacerbated water scarcity, ‘water-tanker mafias’ – dispersed networks of private truck owners, city councillors, farmers, and fixers – siphon groundwater from illicit boreholes and leaky pipes and resell it on the black market for a profit, driving up prices and further stressing water resources.

Figure 4. Country-level water stress in 2040 under the business-as-usual scenario

Wildlife trafficking

One ‘resource’ that will remain a focus for criminal rent extraction is wildlife. Wildlife trafficking is already one of the largest illicit markets, involving nearly 7,000 different species and generating from US$5 billion to $23 billion in revenue. Organized criminal groups are increasingly involved in the trade, which often offers high profits and lower risks than other illicit trades. As global biodiversity declines, more animal and plant products are likely to be protected under domestic or international law, increasing the criminal rents available from trafficking them. Demand for these luxury goods will continue to fuel wildlife trafficking.

“As global biodiversity declines, more animal and plant products are likely to be protected under domestic or international law, increasing the criminal rents available from trafficking them.”

Wildlife products are generally procured in low-income countries, where enforcement is weak, and re-sold in high-income countries for very large profits. Markets in high-income countries in Asia and the Gulf appear to drive demand for a number of today’s most-trafficked environmental goods. Illegal shipments of rosewood, for example, are primarily destined for China and the United Arab Emirates, while an estimated 79 per cent of seized ivory is destined for China.
or South-East Asia. Some of these markets are shaped by long-standing cultural traditions: in China, for example, elephant ivory, tiger parts, and pangolin scales are highly coveted for use in traditional medicine.

Yet increasingly, demand for trafficked products is driven by fads in conspicuous consumption. Rhino horn, for instance, was not traditionally consumed in Vietnam, but in the mid-2000s, it became prized for its rumoured medicinal powers and as a status symbol. Today, the country is one of the world’s largest markets for rhino horn; one kilogramme of rhino horn may sell for as much as US$100,000 – a higher value:weight ratio than for cocaine. Asia, which will likely be home to a number of the world’s largest economies in 2050, as well as a significant percentage of the ultra-wealthy, will likely continue to be the destination for many of these luxury goods. However, a rise in conspicuous consumption among elites in the Gulf, Latin America, and Africa may lead to a diversification of markets. Meanwhile, the growing effects of climate change and related biodiversity loss will likely lead to diminishing supply, driving up prices. The possibility of extinction for some species, such as elephants, pangolins, tigers, and rhinoceros, may disrupt some of today’s largest and most well-known markets.

The gates that control access to these markets are frequently the same ones that control access to other criminal markets: corrupt border guards, for example, do not discriminate amongst the illegal products they waive through. Wildlife trafficking today often converges with other illicit activities, such as trafficking in drugs, weapons, and natural resources, and is closely tied to corruption and bribery of public officials. In Africa, for instance, industrialized elephant poaching seems most prevalent in ‘gatekeeper’ economies, where post-independence elites adopted the rent-seeking behaviour of colonial elites controlling the gate between primary production and external markets. When illicit wildlife trade flows through the same gates used to control drug, human, and arms trafficking, organized criminal groups or corrupt actors that control these population and distribution routes may tax these flows, extracting rents from wildlife smugglers.

As in other markets, state policy choices will be key to determining how and where future rents will be extracted. As certain species are threatened with extinction, national and international efforts to crack down on the illicit wildlife trade may increase. Both China and the United States, for example, have recently banned the commercial trade in elephant ivory. While increased enforcement may help to stem illicit flows, it may also increase scarcity and further drive up prices in specific markets. And governments may turn to other means to control illicit trade, leading to divergent policy regimes. South Africa, for example, recently legalized domestic trade in rhino horn, arguing that it protects the animals, whose horns can grow back if properly removed.

Food and energy fraud

‘Food fraud’, or the repackaging and resale of low-quality or alternate food items as high-quality items, is also likely to increase. This trend is already visible in some markets today: in 2016, Italian police arrested 12 members of the ‘Ndrangheta for selling fraudulent extra virgin olive oil, and in the United States, one estimate suggests as much as two-thirds of the oil sold may be fake or mislabelled. By one estimate, Italian organized crime groups involved in food fraud, known as the ‘Agromafia’, earn US $16 billion annually from this market alone. The proliferation of counterfeit food products may lead to significant market segmentation by price and brand: consumers will pay a premium for brands reputed to have higher supply-chain integrity and security. Closely related, as markets for renewable energy grow, organized criminal groups may also seek to exploit them. Government subsidies designed to encourage investment in and growth of new markets are always attractive to organized crime, and in Italy, the mafia has already moved into the renewable energy market to launder money and garner profits.

Entrance into these markets will allow organized criminal groups to diversify their portfolios, increase profits, and disperse risk. In the market for counterfeit goods, for example, enforcement has been historically weak, offering criminal groups high profits and shorter jail sentences than drug trafficking. One result may, however, be increasingly close ties between professional criminal groups and legitimate corporate entities, with corporate holding entities serving as fronts for a range of legitimate and illegitimate activities. And in some cases, corporate entities themselves may serve as the mechanism for large-scale organized graft and corruption, as we are seeing currently in Latin America with revelations around Odebrecht and the major beef supplier, JBS.

Climate vulnerability and disaster

Climate change will increase the frequency and intensity of extreme weather events, likely precipitating a rise in ‘natural disasters’. The resulting vulnerabilities provide a range of opportunities to criminal organizations and for corruption. First, criminal organizations may step in to provide assistance to vulnerable or impacted populations, as the Yakuza did fol-
lowing the Kobe earthquake, and reportedly may also have done (possibly with tacit state approval) following the Fuku-
shima disaster. This allows these groups to cultivate social support and legitimacy, providing cover for later activities.
Second, criminal organizations may tax third parties who pro-
vide relief and assistance in disaster situations. This is already
evident in some humanitarian contexts. In Bosnia, for exam-
ple, militia leaders controlled the flow of humanitarian aid to
Sarajevo and elsewhere, taxing and plundering shipments. And in Somalia, armed groups have extracted ‘taxes’ from
aid organizations seeking to deliver assistance to millions of
people facing the threat of famine.

Third, criminal organizations can exploit recovery processes.
In the wake of disasters, large amounts of money are often
earmarked for re-construction or public works, offering ap-
pealing opportunities for rent extraction. Criminal groups
that are already involved in the construction or public works
sectors may move in to win contracts, as the yakuza did after
the Kobe earthquake. New forms of organized criminality
or corruption may also emerge in response to large and un-
expected influxes of money. National, regional, or interna-
tional funding intended to help mitigate the effects of climate
change will also be vulnerable to the effects of corruption. A
recent study in Bulgaria found that funds provided for dis-
aster relief following flooding led to more corrupt spending
by local governments. And anti-corruption groups have al-
ready warned about the potential for corruption and waste in
grants made by the UN-led Green Climate Fund, which aims
to finance climate change mitigation and adaptation projects
in developing countries.

Criminal involvement in recovery efforts may also increase
vulnerability to future disasters, as new construction projects
are shoddily completed or left unfinished. In Honduras, for
example, the Cachiros criminal group used front companies
to win contracts for major infrastructure projects following a
tropical storm in 2010. The group reportedly used the con-
tracts to launder approximately US$6.4 million in illicit profits,
claiming projects were supervised by companies that didn’t
exist. Criminal groups executing re-construction or recov-
ery efforts may skirt regulations that are intended to prevent
against future vulnerability – or they may choose not to pro-
vide these services altogether.

Yet the location and scale of the opportunities for organized
crime groups to exploit climate vulnerability will depend sig-
ificantly on how climate change is governed and mitigated
around the world. Poorer and less well-governed communi-
ties are likely to be less resilient in the face of change; cli-
mate change may contribute to spiralling governance chal-
lenges for states and municipal authorities in these regions,
discussed in greater detail below. And climate change may
have significant second-order effects that precipitate disas-
ters, or even armed conflict. There is growing evidence, for
example, that mismanagement of climate-related drought
3. Fragile cities and urban governance

Significant dynamics to 2050: Rapid urbanization, especially in cities already considered ‘fragile’, will likely challenge municipal and state authorities in some regions. Governments may struggle to meet the needs of urban populations, including law enforcement, public infrastructure, and social service provision. Instead, criminal groups may sometimes play these functions, replicating the dynamics currently visible in some urban areas in Latin America and elsewhere. Informal or parallel economies may also emerge, providing new opportunities for rent extraction.

New protection challenges: In some cases, criminal governance may lead to higher levels of violence and insecurity, especially when and where criminal groups compete with each other or with the state for local control. In other cases, criminal groups themselves may establish and enforce norms around violence, and provide protection to individuals otherwise underserved or neglected by the state.

Key implications for governance: The relationship between criminal gangs and state institutions will differ in different regions. In some cases, criminal groups may emerge as direct competitors to state-sponsored governance. In other cases, state or municipal authorities may tacitly allow criminal groups to operate where they are unable (or unwilling) to, or authorities may actively collaborate with criminal groups to provide services and govern urban areas. Criminal groups may also leverage their informal governance power to influence municipal or regional political processes and corrupt elections.

Potential game changers: Widespread adoption of technological advancements disrupts existing models of urban governance and social service delivery (i.e. e-governance, emergence of ‘smart cities’, or increased transparency through crowdsourcing or distributed ledger technology); advances in transportation, virtual reality, and artificial intelligence allow significant portions of the workforce to return to rural living.

By 2050 approximately two-thirds of the earth’s population will likely live in urban areas. Approximately 90 percent of urbanization to 2050 will occur in Africa and Asia, where urban populations are expected to grow by more than 2 billion people. Many of these cities will be littoral – located along coastlines that are especially vulnerable to natural disasters and the negative effects of climate change. The causes and effects of environmental change and urbanization are intertwined: climate change will likely accelerate urbanization, driving rural populations to migrate, while growing urban populations will likely change global consumption patterns and drive up resource use.

Much of the world’s urbanization through 2050 will be concentrated in cities already considered ‘fragile’ – where the state or local authorities are unable or unwilling to provide safety, security, and essential services to residents. Such cities – characterized by an accumulation of risk factors, including unemployment, income inequality, pollution, and violence – are less able to adapt and cope with stress resulting from factors such as unplanned urbanization or climate change. And in these fragile cities, where local and state institutions struggle to meet the needs of the population, hybrid or parallel governing structures often emerge. This creates numerous opportunities for criminal actors.

‘Unplanned urbanization’ and challenges in governance

Between now and 2050, urbanization will occur at a remarkable rate, especially in Africa and Asia, as depicted in Figure 5 (below). The majority of this growth is expected to occur in the world’s least developed areas, often in regions and countries ill-equipped to adequately plan for and absorb large population increases. Rapid ‘unplanned urbanization’ will likely present significant challenges for governance and social structures, especially in littoral areas most vulnerable to the effects of climate change.

As cities grow, governing becomes increasingly complex. This is particularly true in fragile cities, which often ‘exhibit complex hybrid governance structures’. State institutions and municipal authorities often lack the legitimacy or capacity to fulfill core functions for urban residents, including law enforcement, public infrastructure, and social service provision. Informal or parallel economies are also likely to emerge, and as where the pace of urbanization eclipses the creation
of job opportunities in the formal sector. In these areas, local informal actors often serve as intermediaries between the state and the population. Such actors may take a variety of forms, from local gangs to civic associations to businesses to religious groups.

Figure 5. Urban Population, 1990-2050 (millions)

Criminal groups are sometimes said to emerge in these ‘ungoverned’ sections of densely populated urban or peri-urban areas, providing services and protection to local residents. Yet in truth, these spaces are rarely ‘ungoverned’. They are more frequently informally governed, or governed by informal actors with the acquiescence, cooperation, collusion or even collaboration of formal governmental actors, including the state. These informal actors emerge as brokers in informal or parallel economies, and frequently control the gates that connect these spaces and communities to the outside world. As gatekeepers and brokers, they can extract rents – including the protection of criminal activities – for allowing external actors to conduct illicit, or even licit, activities. They may deliver services to communities neglected by state social services, govern informal or parallel economies that emerge, and regulate the allocation of scarce resources. Criminal groups may also play protective roles, controlling the level of violence, dictating community norms, and providing protection to residents by suppressing petty crime.

Organized criminal groups may emerge to control and regulate the extraction of rents in these economies, and to control the gates between local informal economies and larger illicit networks. These groups will become potential brokers of the supply of illicit goods and services, including drugs, arms, and young men and women, into value-chains connecting to richer, better-governed cities in the global north – a pattern already visible in, for example, the role of posses in Jamaica’s garrisons, or family networks in human trafficking from Benin City. In disaster-prone or fragile cities within democracies, such as those in South-East Asia, such groups may also emerge as allies of formal political organizations in controlling the popular vote. Criminal groups may use their governmental reach and coercive power to garner votes and economic support for political groups in exchange for influence and power – as the mafia did in Sicily during the post-World War II transition, and as other criminal groups have in Central America.

Different cities will fare differently. Some of today’s fragile cities may prove more resilient than others, emerging as ‘smart cities’, highly efficient and well-functioning. Such cities will harness developing technology to better manage urban infrastructure, strategically plan for population growth, and embrace partnerships with private actors to effectively and efficiently provide governmental services. Yet others – especially in conflict- or disaster-prone areas – will likely be difficult for local municipal and state authorities to govern, creating opportunities for criminal and corrupt actors. And some of these may become centres of violence.

Violence and the governance of illicit markets

While there is an assumption that illicit markets are more prone to violence than licit ones, the dynamics of violence in illicit markets remain surprisingly murky. It is well understood that because illicit markets exist outside the protection of the law, the groups that operate within them lack access to legal forms of redress – and rely on corruption and violence to resolve disputes and provide informal governance. But high rates of violence are not endemic to all illicit markets. In fact, illicit markets are often relatively peaceful, and the level and scope of violence in different markets and geographies varies considerably. Drug markets in Southeast Asia and Japan, for example, experience much lower homicide rates than drug markets in Central America or Mexico, where they have the highest rates of violence.

Much of the time, criminal groups actively try to avoid the use of violence, preferring not to attract the attention of law enforcement or the media to their other illicit activities. Instead, they may employ violence strategically to achieve specific ends, using force as a selective tool of market regulation in an industry deemed illegal by the state. Violence often increases, for example, when criminal groups compete for control of sites of rent extraction, such as critical drug smuggling routes from Mexico into the United States.
However, state policy choices – and the relationship between organized criminal groups and the state – also play a key role in determining where and how violence will be used in illicit markets. In Japan’s methamphetamine markets, for instance, violence between criminal groups and the state is relatively rare, with both the state and the yakuza employing violence selectively. Richard Friman notes that aggressive enforcement efforts are ‘the exception rather than the rule’; enforcement intensifies ‘when gang activities [cross] what are often vaguely demarcated lines of social order’, such as the spill-over of intergang rivalries into the public domain. States’ choices about how to govern illicit markets are thus an important factor shaping the dynamics of violence in illicit markets.

As a question of how society is ordered and governed, this is an inherently political question. And sometimes the political aspect of these choices impacts formal political processes and institutions. Some criminal groups may choose to use their informal governmental power to influence political processes at the local or national level; occasionally, they even reach across borders. Cockayne has documented, for example, how criminal groups have engaged in cross-border regime change, transnational terror attacks, and rigging of foreign elections since at least the 1950s. More recently, the revelations around the Odebrecht construction company have shown how its Structured Operations divisions deliberately corrupted electoral processes across Latin America.

In turn, states must choose how to govern organized crime. Vanda Felbab-Brown observes that the ‘political management’ of organized crime groups in Southeast Asia, and the way that such groups perceive the state, has resulted in far lower levels of violence in criminal markets than in Latin America. When the state exercises authority and legitimacy over criminal groups, it retains the ability to dictate norms of behaviour: indicating, for example, that while some form of illicit activity is acceptable or tacitly allowed, the use of violence is not. But in states where the government cannot or will not exercise this authority, criminal actors may instead emerge to establish and enforce norms around violence. In the favelas of Rio de Janeiro, in contrast to the situation in similar unplanned urban conglomerations in Asia, some criminal groups have taken on this governmental role in place of the state, regulating certain forms of criminality and violence, such as rapes or unauthorized murders, and arbitrating disputes.

Where and when organized crime leads to outbreaks of violence will depend on many factors. Some states and regions will likely continue to largely retain authority over the use of force and norms of violence. Other states or local governments may choose to accept the presence of certain forms of illicit activity, as long as these markets are not accompanied by outbreaks of violence. Yet other states and regions – especially those where governance is weak, or where the state lacks the legitimacy to enforce norms of violence, may experience more violent competitions for power.
4. Vice markets

Significant dynamics to 2050: Synthetic drugs may come to dominate the global narcotics market, surpassing marijuana, cocaine, and heroin markets in scope and scale. Markets for some illegal goods and services, including drugs, prostitution, and gambling, will likely move primarily (or, in some cases, entirely) online. Individuals may also increasingly use personal or localized 3D printers to download and print illicit narcotics and pharmaceuticals.

New protection challenges: New protection economies will likely form in online markets, as criminal goods increasingly move through digital blueprints rather than hidden in shipping containers or vehicles. Widespread online sales of new forms of synthetic narcotics and counterfeit pharmaceuticals may also lead to supply-chain insecurity and public health risks. Changes in cyber-technology may also alter the opportunities for criminal protection and rent extraction by, for example, facilitating individual, small and medium enterprises’ participation in criminal markets, without relying on larger criminal organizations.

Key implications for governance: Some states may choose to take over the governance of certain vice markets, legalizing, regulating, and taxing the sale of specific goods and services. There may be significant defections, for example, from the global prohibitionist approach to narcotics. Differing regulatory regimes – combined with the move to online marketplaces – will create new arbitrage opportunities, and law enforcement will likely struggle to keep pace with the emergence of new markets and illicit goods (such as new illicit pharmaceuticals or synthetic drugs).

Potential game changers: Development of anti-addiction vaccines; legalization of narcotics; new ‘virtual vices’ completely replace existing markets (i.e., advances in virtual reality narcotic or sex experiences eliminate demand in today’s markets).

Vice markets – markets for criminalized ‘leisure and pleasure’ activities such as drugs, sex, and gambling – will likely remain a significant site of rent-extraction for criminal actors. However, vice markets may look very different by 2050. The production and distribution of illicit goods and services will be disrupted by the same forces distributing other aspects of global production, with organic narcotics increasingly replaced by synthetics, additive manufacturing playing an increased role, automated distribution fleets, the rise of robots and Virtual Reality (VR). Moreover, changes in state policy may fundamentally recast some illicit goods and services – notably marijuana production and consumption – as legitimate, regulated activities, even as new vice markets emerge as states ban or regulate trade in other areas.

Narcotics

By 2050, synthetic drugs may come to dominate the global narcotics market, overtaking marijuana, cocaine, heroin and other ‘organic’ narcotics markets. This will likely be driven both by rising usage of amphetamine-type stimulants (ATS), such as methamphetamine, and the continued emergence of new psychoactive substances (NPS), which mimic the effects of illicit drugs but are often not subject to national or international drug control laws. Both ATS and NPS usage appear to have increased significantly in the past 15 years: ATS seizures increased more than seven-fold between 1998 and 2014, as demonstrated in Figure 6 below, while NPS seizures, although they remain small, increased 15-fold in the same period. New NPS also emerge quickly – between 2008 and 2015, 644 new psychoactive substances were reported to the UN Office on Drugs and Crime and are frequently sold online, marketed as legal highs.

Although today the NPS market remains small and fragmented, larger transnational trafficking organizations may become increasingly involved in this market as demand rises. Criminal groups may also collaborate with licit or semi-licit companies in India and China that produce these drugs in bulk and ship them to markets abroad – possibly forming joint ventures or hybrid companies. Law enforcement may struggle to track and outlaw new substances as they emerge in different regions and markets, creating

“The movement of commerce and social activity online will transform the criminal goods and services being sold, how they are sold, and how groups organize to sell them.”
arbitrage opportunities between different markets.

Figure 6. Trends in the quantities of drugs seized worldwide, 1998-2014


A shift toward synthetic drugs would also significantly disrupt current trafficking routes and change the sites of rent-extraction. Today, the vast majority of coca and poppy is cultivated in just a handful of countries, but synthetic drugs may be produced anywhere. The internet has allowed the development, production, and marketing of synthetic drugs to proliferate, and increasing licit trade, especially to and from Asia, has created opportunities for illicit trade as well. Globalization will likely continue to facilitate both the movement of necessary precursor chemicals and the transfer of knowledge across borders – in Nigeria, for example, Mexican drug traffickers have reportedly helped traffickers set up meth labs and trained them in production techniques.

Technological advances will further alter the geography of narcotics markets. By 2050, individuals may be able to easily download blueprints for pharmaceuticals and synthetic narcotics, and produce them on personal 3D printers. Trafficking organizations may seek to control both the physical distribution of raw materials and the online distribution of cyber-blueprints. Changes in global transportation – from the emergence of new shipping routes due to climate change to the widespread prevalence of unmanned vehicles – will also alter the flow of both licit and illicit trade.

The changing geography of drug production may also track shifts in drug consumption markets. The presence of drug production or transit in certain regions may be correlated with increased domestic consumption (although it is not clear which way causality may flow): in China, for example, synthetic drug use has risen as domestic production has increased. Similar trends can be seen elsewhere – in Europe, which has become a major producer of amphetamines, methamphetamines, and cannabis, many of the drugs produced in the region are also consumed there. And although methamphetamine trafficked through or produced in West Africa is primarily destined for high value markets in Europe or Asia, domestic consumption also appears to have increased in recent years. At-home or localized 3D printing of synthetic narcotics and pharmaceuticals may further contribute to these shifts, leading to increased consumption of certain drugs in regions where they were previously unavailable or relatively rare.

Virtual vices

The movement of commerce and social activity online is likely to transform vice markets in significant but complex ways: what is sold, how, and how groups organize.

First, it is transforming the cost and organizational structures of markets for illegal goods and services. Although online trade is still a small segment of global drug sales, online sales of illicit narcotics increased by more than 900 percent between 2012 and 2015. Synthetic drugs, in particular, are a growing segment of the online marketplace. They are less bulky than cocaine or heroin, making them easy to ship long distances. The online marketplace enables dealers to more easily take advantage of arbitrage opportunities created by different regulatory regimes; much of the illicit supply of synthetic opioids, for example, is produced in China or elsewhere in Asia, where precursor chemicals are ‘either legal or easier to procure’, then shipped to the US or Europe. The ease and relative anonymity of online commerce is also transforming markets for licit, but regulated, pharmaceuticals, facilitating consumer circumvention of regulatory checks. The growing online sale of medicines, for example, has allowed for the widespread internet-based distribution of unlicensed prescription drugs, painkillers, and performance-enhancing drugs, as well as counterfeit, falsified, or substandard pharmaceutical products.

Online drug sales may also create opportunities for rent extraction in new markets or lead to growth in previously small markets. Prices for street drugs in Australia, for example, are traditionally three to four times higher than in other high-income countries, due to the country’s geographic remoteness and relatively strong border security. But unlike in other high-income countries, narcotics in Australia sell for less online than they do on the street; the online market opens new arbitrage opportunities, allowing a dealer to buy street drugs at a low price in Europe, for example, and ship them to buyers in Australia. Drugs can be resold for such a significant mark-up that dealers are willing to take the risk of the package being intercepted by customs.

Digital marketplaces and platforms are also reducing the
costs of entry into other illicit markets: individuals can more easily create market their own sexual services online, for example, potentially limiting possibilities for rent extraction by brokers or intermediaries.150 Groups may use both the dark web and the surface web to sell prostitution: sites on the ‘deep web’, for example, have been used to recruit and market human trafficking victims, while the mafia has used Craigslist to facilitate interstate sex trafficking in the United States.151 These online marketplaces present significant regulatory and detection challenges for law enforcement, often spanning different jurisdictions or crossing state borders, and allowing participants to use encryption or anonymous profiles to disguise their activities.152

Second, the digitization of social life will generate new virtual vices, which take place wholly or largely online or with robots, including virtual sex and online gambling. Just as the advent of the internet (and permissive regulatory policies towards it) fuelled the growth of the multibillion-dollar online porn industry, new technologies will continue to open up new possibilities: virtual reality and connected devices have already been used on ‘camming sites’, websites where users can pay to watch individuals perform sex acts while they chat with them.154 The online gambling industry is also growing rapidly: currently worth more than US $30 billion, its value is expected to nearly double by 2021.155 In FY 2015–16 in the UK, the online gambling market generated £4.5 billion, making it the largest segment of the British gambling market.156 By 2050, entirely new digital vices are likely to emerge. In Japan, for instance, ‘romance gaming’ has become a significant segment of the online gaming marketplace; approximately 30 per cent of single women and 15 per cent of single men between age 20 and 29 admitted to falling in love with a meme or character in a game.157

Some of these new digital vices will be banned in some places, but not others, creating both arbitrage opportunities and policing challenges. As with other cybercrimes, criminals can base their activities in markets where such activity is legal or enforcement is weak, and serve customers in regions where the market is banned. Law enforcement is also heavily reliant on private sector actors, from online gambling or pornography sites to internet service providers, to police access to these markets.158 But in some cases, states may adapt to take advantage of these opportunities – legalizing, regulating, and taxing certain vice markets to increase revenue. Today, for example, more than 80 countries have already legalized online gambling.159 Once again, state policy choices will be crucial in determining outcomes.

States make crimes

States define what is criminal in law, and what is permitted in practice. The policy choices made by states will therefore shape the way that vice markets develop and the protection, arbitrage and rent-extraction opportunities available to criminal organizations. Markets that are now considered criminal may, in some parts of the world, be taken over by governments, who will regulate and tax these markets – making criminal rents licit, as some states have done with alcohol, gambling, or tobacco – while new regulations in areas such as luxury wildlife products may lead to new markets.

For example: by 2050, there may be significant deflections from the global prohibition on narcotics will, by 2050, lead to significant differences in narcotics regulation. This will create significant protection, rent extraction and arbitrage opportunities.”

Drug markets could also be significantly disrupted or stymied by technological or research advances available to and shaped by state policy, licensing, funding and regulatory choices. Vaccines may prevent addiction to drugs such as nicotine and cocaine, or genetic sequencing may be used by states or law enforcement to determine predilections for drug dependency and target prevention efforts at specific individuals.164 Non-addictive psychedelic drugs or chemically-enhanced virtual reality experiences may emerge, sanctioned by states, which could displace the more risky experience of unregulated, illegal narcotic consumption.165 Yet the implementation of such advances is likely to be costly and fraught with ethical or political concerns – meaning some states may choose to implement technology-based reforms, while others may be unwilling or unable to do so. How states make these choices will define what is criminal in law, and in reality. States, ultimately, ‘make’ crimes.
5. Cyberpower

Significant dynamics to 2050: With the majority of human activity captured online, data will be increasingly vulnerable to theft, fraud and extortion – creating new demands for protection and new opportunities for criminal organization and governance. Some criminal organizations will likely seek to exploit cybervulnerabilities to extract criminal rents, and individuals, businesses, and government institutions may face increasing insecurity. This, in turn, will lead to new models of protection, as state, private, and criminal actors compete and collude to provide security against new cyber-risks. Cyberspace will also provide a new medium and venue for criminal organization, with relatively low barriers to entry and low risk of detection, disruption and punishment. These dynamics will, however, depend in large part on how states and private actors choose to build and regulate the internet as it evolves.

New protection challenges: Cybervulnerability will drive demand for protection for individual, corporate, and government actors. Low-level cyber-criminality may become increasingly widespread, especially in countries where economic opportunities in the licit economy are limited. Increasingly, every industry will be vulnerable to attack – leading to a myriad of protection challenges in everything from healthcare to agriculture. Trust services and effective quality control in digitized business processes and cyberspace, rather than physical protection or real property integrity, will become increasingly important. Virtual protection rackets may emerge, and both state and private actors may collude with criminal actors to provide protection or exploit vulnerabilities.

Key implications for governance: Cyberspace will increasingly be a source of governmental power, and the governance of cyberspace is likely to be increasingly contested. New forms of competition and collusion will emerge between governments, private companies, and non-state actors, who will view cyberspace as a way to extend their coercive power and strategic reach. Some states may attempt to provide highly protected and surveilled safe spaces for their citizens, while others may actively collude with cybercriminal groups, using them as proxies to achieve strategic aims. Criminal groups themselves may emerge in the governance of certain corners of the internet. Divergent policy approaches may create new arbitrage opportunities for criminal actors, who may deliberately organize their activities from states or online platforms where regulation or enforcement is weak.

Potential game changers: Widespread insecurity leads to declining global internet usage; major geopolitical conflict in cyberspace (i.e. development of ‘digital nuclear weapons’, attacks on space-based satellites); sequestration of cybercapabilities into separate cyberdomains; advances in quantum computing make networks impenetrable to hackers.

“Cyberpower – the ability to subordinate cyberspace and control digital data – is supplementing biopower – the ability to subordinate bodies and control populations – as a source of governmental power.”

As we saw in the previous section, vice markets are being significantly reordered by their move online. But cyberspace is also a medium through which increasingly valuable data travels, a vector for coercion (think distributed denial of service (DDOS) attacks; WannaCry ransomware; and StuxNet-style cyberattacks); and a medium for knowledge exchange and social (including criminal) organization.

As cyberactivity is increasingly seen as vulnerable to theft, fraud and extortion, cyberspace is becoming a venue for protection, and, fast on its heels, the emergence of new criminal organizations and governance. Today, cyberspace functions like a global commons, even though it is in fact an artefact of corporate- and state-controlled infrastructure; by 2050, this may have changed, if states, businesses, or non-state actors seek to wall off portions of the internet, within which to offer ‘protection’, just as early modern European princes walled themselves off into sovereign ‘states’. And increasingly, cyberpower – the ability to subordinate cyberspace and control digital data – is supplementing biopower – the ability to subordinate bodies and control populations – as a source of governmental power.

Our lives are increasingly cyber-connected. Everything from telephones to hospitals to nuclear weapons is now networked through the internet. Organized crime is no different.
Exploiting cybervulnerability

Digital data collected by private companies and governments is increasing exponentially, as more and more social, commercial and political activity is carried out through digital and cyber-enabled devices – not just the ‘internet’, but also the ‘Internet of Things’. In 2000, only a quarter of the world’s information was stored digitally; today, it is more than 98 per cent.\(^1\) By one estimate, the digital universe doubles in size every two years.\(^2\) By 2045, as many as 50 trillion everyday devices may be connected to the internet.\(^3\) The data generated by these devices will be enormous; in 2014, the data generated by sensors connected to the Internet of Things accounted for 2 per cent of the digital universe – by 2020, it may rise to 10 per cent. This will affect virtually every industry, from health care to manufacturing to agriculture to transportation.\(^4\) Just one driverless vehicle may produce 4,000 gigabytes of data a day.\(^5\)

In a world that is permanently online, digital footprints and signatures are highly valuable commodities, and organized theft of this information is increasingly big business. Cybercrime is estimated to cost US$400 billion a year; by 2019, costs may reach US$2 trillion.\(^6\) The lines between the licit and illicit marketplaces for personal data will likely be increasingly blurred, as both criminal groups and legal ‘data brokers’ buy and sell personal data in online exchanges.\(^7\) Biometric and other highly personal data are also increasingly likely to be held to ransom. Ransomware attacks, by one estimate, increased by 166 percent between 2015 and 2016 alone.\(^8\) The May 2017 ‘WannaCry’ ransomware attack affected more than 230,000 computers in over 150 countries – including 48 National Health Service organizations, affecting health-care delivery to thousands of patients.\(^9\) The attack highlighted the vulnerability of a range of devices and processes to hacking and extortion, raising concerns about how susceptible the Internet of Things may be to hacking and ransomware, and the impact hijacking could have on average citizens’ lives – from hijacked cars to disrupted surgeries. Cyber-attacks have already moved beyond mere ‘nuisance’ and are now used to perpetrate crimes with much larger profits, such as stealing bank passwords or committing internet-related stock fraud,\(^10\) and much more significant political and social consequences, such as recent hackings that have influenced elections\(^11\) and disrupted power grids.\(^12\)

Today’s ransomware attacks will likely appear rudimentary and antiquated by 2050 – but the question of cybervulnerability will remain central. Individual data, such as data from medical devices or online activity, and network data, such as data from transportation systems or critical infrastructure, will increasingly be automatically collected and stored, leaving it vulnerable to theft, destruction, or ransom. In addition, as more industries become automated and artificial intelligence-driven decision-making becomes more prevalent, such attacks may have even greater consequences. The agricultural sector, for example, may be increasingly cybervulnerable as farms increasingly rely on digital data and sensors to monitor crop growth and improve agricultural efficiency, and production systems become more automated and autonomous.\(^13\) Networks are generally most vulnerable when new technologies are grafted onto legacy systems, posing particular threats for industries with large, outdated technological systems, such as the healthcare, educational, and agricultural sectors.\(^14\) This also raises significant challenges for governments; some states will likely struggle to update critical technical infrastructure or upgrade cybersecurity capabilities, leaving them especially vulnerable to cyberattacks.

Cyber-protection

These cyber-vulnerabilities in turn create demand for cyber-protection. Much of this is provided not by state actors, but by private, commercial actors: by 2020, the global cybersecurity market is expected to be worth US$170 billion.\(^15\) Of course, these figures reflect the market to protect licit cyberactivity; illicit cyberactivity requires its own cyber-protection. Online protection racketts appear to be increasing. At the same time, businesses, states, consumers and private actors increasingly differentiate between the types of data that require protection and the risks they are willing to bear and the price they will pay for protection. They may also be willing to engage in more conscious choices around data security, for example agreeing to increased control of data by internet service providers and online platforms in return for increased protection of that data from third parties.

States seem quite likely to choose, in the next thirty years, to become more active in providing cyber-protection. This could take a variety of forms. One approach may involve sequestration, with governments providing controlled ‘safe’ spaces – essentially walled-off enclaves – within which online activity is highly protected, but also potentially highly surveilled. This could be understood as an attempt to expand the Westphalian model to cyberspace.\(^16\) The physical gates by which citizens access the internet are already an important site of contestation of governmental power, with countries such as China and Iran seeking to extend their physical borders into the digital, monopolizing control over the way their citizens access the internet and receive information.\(^17\) (This may be complicated by the rise of satellite-provided internet access.) Fibre optic cables are also key elements of access to cyberspace: some countries use deals with private companies, and physical breaches, to monitor and hack global internet traffic.\(^18\) Private actors may soon get in on the act.\(^19\)

Another approach may be for states to support the creation of open, but nonetheless highly protected, spaces and services, for example by agreeing to protocols that require service-providers to meet certain data security protection standards. Germany, for instance, has used its G20 presidency to raise discussions about unified digitization policies.\(^20\) Such
an agreement could take a number of different forms. States may choose to cooperate on a global level, for example, working with private cyberinfrastructure providers to establish international standards that ensure collective protection in cyberspace. Or different states and municipalities may form bilateral partnerships with business and economic actors, creating closed-off, protected cyber-networks where protection and trust services are provided to specific populations.

And third, states may engage in more covert protection activities – offering cybercriminals sanctuary and protection, in return for tribute or allegiance. A recent European Council on Foreign Relations report suggests this is how the Kremlin currently deals with Russian-based organized crime elements in Europe, and there are signs other countries may also be taking this approach. State collusion with cyber-criminals will blur the lines between cyber-surveillance, cyber-subversion, and cyber-warfare. Small states – or even corporations, non-state organizations or individuals – may seek to use cybercrime as a force multiplier.

But complete state control of cyberspace is unlikely, not least because key parts of the infrastructure of cyberspace are produced, distributed, owned and operated by private commercial actors. In those spaces that are more weakly controlled, criminal groups themselves may emerge as providers of cyber-protection, establishing and protecting cyberspaces for criminal interaction and organization, as we discuss further below.

“States, corporations, non-state organizations or individuals may use cybercrime as a force multiplier.”

As states and other actors that help to regulate cyberspace take different approaches, this will present organized crime with significant arbitrage and protection opportunities, just as different regulatory approaches in physical territory do. Criminal actors will likely deliberately organize their activities from states or online platforms that offer them maximum opportunities and minimum constraints – weaker states, for example, or states or online platforms with laxer controls.

Hacker crews and cybermercenaries

Cyberspace provides a new medium and venue for criminal organization, with relatively low barriers to entry and low risk of detection, disruption or punishment. Even sophisticated crimes, such as hacking or fraud, come with relatively low barriers to entry – often just the price of a computer and an internet connection, with user-friendly malware increasingly widely available. There are signs that low-level criminality – piracy, intellectual-property theft, identity fraud and online ransoms – may become commonplace, but also come to be seen as relatively low-impact and routine. As more individuals in low-income countries gain internet access, and as automation leads to diminishing job opportunities in some regions, cybercrime may become increasingly attractive and ubiquitous. The way in which these forms of criminality and criminal organization evolve in the future will depend on how the internet itself evolves. Distributed ledger technology, for example, may enable significant decentralization in the financial industry, with no central authority responsible for coordinating and processing transactions. Opportunities for large-scale internet fraud or theft, such as last year’s multimillion dollar theft from the Bank of Bangladesh, may decrease – instead, we may see a rise in low-value cybercrime that targets end users.

We already see the emergence of cyberspaces within which criminals are coming together to form job-specific ‘crews’ and ‘sets’, and a transition to a ‘crime-as-a-service’ business model. Darkode, for example, is a cybercrime forum where criminals can ‘trade and barter their hacking expertise, malware, and botnets, and… find partners for their next spam runs or malware attacks’.

Cybercriminals are relatively easy to find and hire, and we may be seeing the emergence of bands of cybermercenaries for hire. Some, with close ties to particular states, may be de facto arms of those states, but able to be loaned to foreign states – for a price. There are some suggestions, for example, that cyberattacks on Al Jazeera and other Qatari organizations in June 2017 may have been carried out by Russian hackers, perhaps with the permission or acquiescence of political handlers and masters.

By 2050, cybercriminality is thus likely to be highly fluid, and not confined to defined, specialist organizations – though those will exist. Governments, businesses, and non-state actors may all see cybercrime as a way to extend their coercive power and strategic reach, further blurring the lines between legitimacy and criminality.
6. Follow the money

Significant dynamics to 2050: Changes in the way value is stored and transferred will create new opportunities for the capture and movement of criminal rents. Digital financial systems may be increasingly targeted for attack, and cryptocurrencies will also create new opportunities for tax evasion and money laundering. Illicit financial flows will likely remain an important component of the global political economy, even as the vectors and mediums for those flows may change. And in some parts of the world, large-scale and sustained corruption may perpetuate inequality and lead to political and social insecurity.

New protection challenges: High levels of corruption and illicit financial flows in many parts of the world will continue to undermine state service provision and exacerbate inequality and insecurity, opening space for criminal actors. New protection needs will also arise to guarantee the safety and stability of virtual currencies not backed by state institutions – and the corresponding financial volatility may threaten the macroeconomic stability of some states or lead to new forms of insecurity. But adoption of new technologies, such as distributed ledgers, may also increase transparency and security in some financial systems.

Key implications for governance: Illicit financial flows are made possible in part by regulatory policy choices and governance arrangements, especially as they relate to bank secrecy, non-disclosure of beneficial ownership, and tax haven arrangements. Efforts by states to strengthen global regulation and enforcement may diminish opportunities for illicit value transfers, and for corruption. But such efforts will be challenged by the prevalence of virtual currencies and other e-money systems, which prevent significant regulatory and enforcement challenges for states, and will require high levels of international cooperation. By 2050, the shift from fiat to virtual currencies may also weaken states’ control over revenues, monetary policy outcomes, and macroeconomic stability. New forms of economic governance may emerge instead – for example, states, municipalities and private actors may cooperate to create closed-off and highly secure value-transfer systems.

Potential game changers: Global adoption of distributed ledgers leads to significant advances in financial transparency; financial crisis or collapse accelerates decline of fiat currencies; economic dissatisfaction and perceptions of corruption leads to large-scale conflict in multiple states; high-profile corruption scandal leads to regime collapse or fall of major transnational corporation.

The geography and organization of crime and corruption depend significantly on where and how value gets stored and transferred; this is why, famously, investigators ‘follow the money’. Organized criminals and corrupt officials rely on value transfer systems both as targets for rent extraction (think: robbing banks), and as mechanisms for themselves moving, hiding and protecting wealth (think: money laundering). How value gets stored and transferred is likely to change significantly by 2050 – with significant implications for how crime and corruption are organized.

Crime changes with payments and storage systems. Bank robbery used to involve attacks on physical branches and their vaults; now, online attackers attack multinational financial systems. In 2016, for example, a cyberheist allegedly linked to the North Korean government illegally transferred US $81 million from the Bangladesh central bank.200 Similarly, innovations in the regulation of casinos and gambling in America in the nineteenth and twentieth centuries made them key targets for organized crime. As commercial airline travel put offshore banks and casinos within easier reach, the geography of money-laundering and thus organized crime changed significantly, creating the basis for today’s ‘off-shore’ financial system.201 Changes in relative values also impact how criminal proceeds get stored and transferred. Real estate booms often attract illicit proceeds (think – ‘safe as houses’).202 And in recent years, the euro (€) replaced the dollar ($) in gangsta culture as a sign of wealth, because of the high weight:value ratio of the €500 note.

The digitization of finance represents the next iteration in this evolution. In this section, we consider how illicit financial flows are likely to develop over the next three decades, and then consider how changes in value transfer systems, including
the emergence of non-monetary systems such as distributed ledgers and closed credit networks (loyalty alliances) may influence and change money-laundering altogether. Because they represent a movement away from state-backed currency systems towards systems in which private actors play a stronger governmental role, they potentially represent a step-change in how wealth – and therefore power – circulates globally.

Illicit financial flows

The concept of ‘illicit financial flows’ as currently used refers to several different things, including:
- the movement of money obtained illegally (e.g. through corruption or organized crime);
- the movement of funds whose source is legal, but whose transfer (through tax evasion or money laundering) and/or intended use (for purchase of criminalized goods, for bribery, for terrorist financing purpose) is illegal; or
- financial flows that are notionally legal (i.e. not illegal), but which appear to occupy a legal grey area ‘between compliance and [tax] evasion’.203

The cumulative size of these flows is substantial: in 2014 alone, illicit financial flows from developing countries were estimated at nearly US$1 trillion.204 In a number of developing countries, these flows are estimated to be more than 10 per cent of GDP,205 or even higher percentages of total national wealth.206 Although illicit financial flows affect both developed and developing countries, the effects of illicit financial outflows are particularly acute for developing or emerging economies, especially as a percentage of total economic activity.207 Recent high-profile corruption scandals further illustrate the scope of the challenge: in Malaysia, for example, senior officials are alleged to have used a sovereign wealth fund to divert more than US$1 billion into Swiss bank accounts.208 A recent Transparency International report estimated that former Nigerian military leaders stole approximately US$15 billion from the state through fraudulent arms procurement deals.209 Sub-Saharan Africa, in particular, appears to experience higher illicit financial outflows as a percentage of total trade. From 2005 to 2014, outflows were estimated at 7.5 per cent, compared to 4.6 per cent for all developing countries.210 Outflows are often closely tied to resource rents, suggesting resource governance will remain a central concern.211

These flows are made possible in significant part by regulatory policy choices and governance arrangements, especially relating to resource governance, bank secrecy, non-disclosure of beneficial ownership, and tax haven arrangements. Some of these policies are, in turn, the product of emphasis on capital mobility and financial globalization over the last three decades. Liberalization of foreign exchange regulations in the 1980s increased capital mobility, but also led to the emergence of new tax havens.213 By one account, the world now has anywhere from 50 to 60 active tax havens, primarily located in the Caribbean, parts of the United States (such as Delaware), Europe, South-East Asia, and the Indian and Pacific Oceans,214 and anywhere from US $21 to $32 trillion may be invested in ‘offshore’ tax jurisdictions, a conservative estimate that omits ownership of real estate, yachts, gold, and other products used to disguise illicit gains.215

There are, however, signs of a move by some states to strengthen global regulatory and enforcement coordination. If this continues, we can anticipate that this will lead to more creative forms of illicit value transfers. High-value commodities such as art, luxury vehicles, or real estate, for example, may be increasingly central to corruption and money-laundering. These markets have, in recent years, emerged as significant conduits of IFFs, often in cases of grand corruption,216 and will likely continue to serve as a parallel channel to the formal financial system. Increasingly, however, we are likely to see a greater reliance on digital solutions. The rise of digital finance has already factored into illicit financial flows, making it easier to transfer money, set up shell companies, and maintain offshore accounts.217 New digital currencies and value transfer systems (discussed further below) may herald even more change.

The smart money?

The monopolization of the power to recognize, license, and often issue, legal tender has been a central feature of modern states.218 But states have not always been the only players in this space: until well into the twentieth century, bank notes were issued, as the name might suggest, by private banks – leading to significant financial volatility, speculation and outright fraud. It was only in 1913, for example, that the US Federal Reserve was granted the monopoly on issuing notes,
and it took another 20 years for them to become the sole legal tender. Today, private actors are central to a range of both formal cross-border value transfer systems (such as correspondent banking relationships, remittance corridors, and the SWIFT system), and informal systems (notably the hawala system). And globalization has significantly altered the geography of money in other ways, with growing inter-penetration of national monetary systems.219

By 2050, state control of monetary systems may be further weakened, in particular by the emergence of ‘virtual currencies’ - private sector systems that, in many cases, facilitate peer-to-peer value transfers bypassing traditional central clearinghouses. The term ‘virtual currencies’ (VCs) covers a wide array of digital representations of value, ranging from ‘cryptocurrencies’ such as Bitcoin to Internet and mobile coupons to airline miles.220 VCs are closely related to ‘digital currencies’, which include e-money systems that are tied to fiat currency (legal tender backed by an issuing state government). Unlike systems such as Venmo or PayPal, virtual currencies are not denominated in fiat currency and have their own unit of account.221

The value of both virtual currencies and digital currencies is growing. Bitcoin has a market capitalization of US $11.4 billion, up from US $1 billion in 2013.222 And the combined value of Bitcoin and Ether, the two largest cryptocurrencies, is approaching the market value of Goldman Sachs.223 Less prominent value-transfer systems have also grown: the airline-miles reward system, for example, which functions as a non-monetary value transfer system, now accounts for more than half of all profits for some of the largest American-based airlines.224 And cyber-enabled peer-to-peer payment systems – from Venmo to bank-owned payment systems, such as Chase QuickPay – also handle an increasing share of all payments. More than 30 US banks and credit unions, for example, just rolled out a unified peer-to-peer payment system to compete with Venmo, which processed US $17.6 billion in 2016.225

A recent International Monetary Fund study found that virtual currencies are particularly hard to regulate, and provide new opportunities for organized crime, money-laundering and terrorist financing. VCs are often opaque, enabling greater anonymity than other non-cash payment methods, such as credit cards. The sender and recipients may not be adequately identified, making transfers difficult to trace.226 This anonymity has made them the ‘currency of choice’ in some cyber-related criminal activity, from the purchase of drugs on Silk Road to the payment of ransoms in the WannaCry attack.227 Decentralized virtual currencies, such as Bitcoin, which is underpinned by a distributed ledger system, are particularly appealing for criminal actors: ‘by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider’.228

The transnational nature of VCs also makes them difficult to regulate. Virtual currencies allow for rapid and easy cross-border payments over the internet or by mobile phone. Cryptocurrencies in particular may also facilitate tax evasion, as market participants do not need to disclose their identity, even when sending money overseas. In addition, payment systems may be built on complex infrastructure that spans multiple jurisdictions, leading to a lack of clarity on responsibility for anti-money laundering compliance and supervision.229 Different jurisdictions have regulated the use of VCs in different ways. Some countries, such as Bolivia and Russia, have banned their use altogether, while others have yet to issue formal regulation.230 This, of course, will lead in time to arbitrage opportunities.

At present, regulators are primarily targeting the ‘gatekeepers’ to VC systems, including VC market participants and the financial institutions who interact with them.231 This system of regulation is currently possible because VC users generally need to ‘cash out’, turning their VCs into fiat currency. But the IMF envisages that this may become increasingly difficult, and when the systems evolve into peer-to-peer mechanisms, and users spend more of their time (and value) ‘inside’ the network than outside.232

Over time, this will have macroeconomic impacts for states. As more financial value transfers away from fiat currencies to VCs, state revenues and monetary policy leverage may be impacted.233 These macroeconomic impacts will likely be further compounded by the decline in dollar hegemony; increasingly, there will be a broader set of both fiat and virtual currencies that exert significant currency influence.234 There are also initial concerns that fixed-supply cryptocurrencies could be vulnerable to structural deflation, as the gold standard was nearly a century ago.235

Future efforts to regulate VCs, and digital currencies more broadly, will require high levels of international cooperation. Some coordination is already evident: both the Financial Action Task Force and the UN Office on Drugs and Crime, for example, are increasingly considering questions of prevention and response to the money-laundering risks posed by VCs,236 although the larger social, economic and developmental implications of VCs have not yet been carefully considered. But full coordination will require states to agree, at least broadly, on the benefits and risks posed by these alternate currencies, as well as how to classify them.237 Coordination with private sector actors may also be key, as regulators require new technology or access to monitor and investigate VC transactions.238 In lieu of global cooperation or governance, new arrangements may emerge. States, municipalities
and private actors, for example, could partner to create new, protected economic networks — in which highly secure, sanctioned VCs facilitate free trade and digital commerce in designated economic zones.

**The ‘corruption trap’**

Whatever the vector for illicit financial flows in 2050, there is a growing realization that, over time, such flows contribute to the erosion of the legitimacy not just of the specific actors that are engaged, but the politico-economic systems that enable such large-scale and sustained corruption. The system itself begins to be seen as hopelessly ‘rigged’ and corrupt, serving ‘not the many but the few’ — the infamous ‘1 per cent’. There is also growing evidence that corruption and inequality are closely related — and, indeed, feed off each other. By 2050, these dynamics may, increasingly, lead states off the path of sustainable development and into a ‘corruption trap’, perhaps even more pernicious — for being slow-onset and therefore less remarkable — than Paul Collier’s famous ‘conflict trap’.

The prevalence of large-scale corruption is, of course, difficult to measure — like organized crime, corrupt actors are inherently interested in keeping their activities secret. But many scholars believe that neoliberal globalization’s favouring of capital mobility over labour mobility and social protection measures has led to an increase in levels of corruption around the world. Certainly, public awareness of and anger about corruption appears to have grown significantly in the past 20 years. Corruption is consistently cited by citizens of emerging and developing nations as one of the top problems facing their countries. A 2014 survey by Pew Research Centre found that a median of 76 per cent of people across 34 developing economies said that corrupt political leaders were ‘a very big problem’ in their country, up from 63 per cent in 2007. Corruption is increasingly cited as a pressing concern in developed countries as well: in 2014, three-quarters of respondents surveyed by the European Commission said that corruption was widespread, and more than half believed the level of corruption had increased. Global protests have also increased; more than 60 countries, in every region of the world and in every type of political context, experienced major citizen protests from 2006 to 2016. And unlike the protests of the 1980s and 1990s, which were often focused on transnational issues such as globalization, protests are increasingly driven primarily by specific and local economic and political grievances relating to corruption.

An increase in perceived inequality has helped to fuel perceptions of growing corruption and citizen dissatisfaction with government, especially since the 2008 financial crisis. Wealth is increasingly perceived as being concentrated in the hands of fewer people; today, the bottom 50 percent of the world’s population owns less than the richest 85 people in the world. While these gains are, in many cases, not necessarily the result of corruption, increased concentration of wealth has fuelled the perception that the ‘system is rigged’ to benefit elites at the expense of the poor and middle class. An Oxfam survey across six countries, for example, found that a majority of people in each country believed that laws were skewed in favour of the rich. ‘Corruption’ has become shorthand for the power, impunity, and wealth that have accrued to global elites, increasingly reflecting a ‘general pattern of civic anger about how state power is exercised’.

And indeed, there is increasing consensus that corruption and inequality are correlated — and that each plays a role in reinforcing the other. Widespread corruption may lead to inequality in multiple ways: it often hampers economic development, slowing the rate of poverty reduction; leads to diminishing state revenues due to graft and tax evasion; and diverts money from social services, education, and other programs targeted at the poor. And high levels of inequality may perpetuate corruption. The gains from corruption often accrue to the rich and well-connected, especially as elites implement policies or regulations to further the benefits they receive from the system, while the poor may be more likely to be exploited. Grand corruption also seems to beget petty corruption: a recent study published in Nature seems to demonstrate that the perception of governmental corruption increases normal citizens’ willingness to participate in corrupt and dishonest behaviour even in private transactions.

Figures 8 and 9 below point to the correlation between social exclusion and corruption. They map scores on Transparency International’s Corruption Perception Index to two indicators of social exclusion (differentiated because there was no single measure for OECD and non-OECD countries). Higher scores signify less corruption/exclusion.

**Figure 8. Corruption and Social Exclusion in non-OECD countries**

There is also growing consensus that corruption is a significant driver of political instability and state fragility. Sarah Chayes, for example, argues that governments’ increasing turn to systemic corruption – ‘a methodical purposing of government functions around the objective of extracting resources to enrich ruling networks’ – undermines the legitimacy and security of the state in multiple ways.

What are the vectors by which corruption and large-scale organized crime undermine development?

First, corruption weakens the effectiveness of state institutions, diverting resources to state elites rather than to the provision of social services or protection. Military budgets, in particular, are particular targets of corruption: in Nigeria, for example, large-scale graft – on the order of more than US $15 billion – has left the military ‘without vital equipment, insufficiently trained, low in morale and under-resourced’ in its fight against Boko Haram. In Mali, systematic corruption and patronage helped to fatally undermine military effectiveness, leaving the state ill-equipped to respond to the emergence of AQIM. Similar cases can be made for military weakness in Iraq, Ukraine and Afghanistan.

Secondly, systemic or grand corruption undermines the social contract between citizens and the state. State institutions are bent to funnel criminal rents into the pockets of national elites, rather than to provide social services and protection to citizens. And widespread corruption – both grand and petty corruption – also breeds resentment. Individuals who are repeatedly taken advantage of, humiliated, or injured by the actions of corrupt government officials – usually without recourse – lose their faith in the willingness or desire of the state to act in their best interests.

Third, there is growing evidence that communities with significant organized crime presences risk becoming ‘junky economies’, suffering a kind of Dutch disease in which economic inputs (labour, capital, land) are slowly sucked (or coerced) into criminalized livelihoods and enterprises. Small and medium enterprises become zombies for criminal activity. With workers deskillled and populations increasingly dependent on illicit income sources, struggling in the trap just seems to make things worse.

These dynamics open space for alternate providers of governance – including organized crime, insurgent, or terrorist groups. In this space, these groups may emerge not just as providers of social services and protection, but increasingly, as purveyors of norms, meaning, and culture. Individuals who no longer feel protected by the governing apparatus of the state may place their loyalties elsewhere – overtly or, in the case of organized criminal groups, covertly. And while not all criminal groups will take on this governmental role, those that do may use their power to further weaken the authority of the state. Corruption also combines with other risk factors to increase insecurity. These risk factors include proximity to criminal or terrorist networks; horizontal inequalities; social conflict; and, potentially, governance challenges posed by climate change or environmental damage.

And high levels of corruption seem to correlate with the presence of political instability, violence, and terrorism, as demonstrated in Figure 10 (overleaf) – though this does not, of course, speak to the direction of causality.

The Arab Spring provides perhaps the most visible example: from Tunisia to Syria, endemic corruption and abuse by political elites were a major motivating factor behind the protests and calls
for regime changes. But corruption also played a key role in civil unrest in Ukraine and Kyrgyzstan, and has helped to fuel insurgencies in Nigeria, Afghanistan, Mali, and beyond. The Carnegie Endowment’s Working Group on Corruption and Security found that 50 different countries experienced ‘corruption-related security incidents’ between 2008 and 2014, including sudden regime change or war due to anti-kleptocracy protests, serious violence due to corrupt alliances with trafficking networks, insurgency or coups traceable in part to outrage at corruption, severe electoral violence sparked by corruption, and widespread popular protests or coup attempts against corruption.
Policing is not simply a question of enforcing law, but also of providing protection. If and as private actors become increasingly central to the provision of the spaces and systems in which social, economic and political activity take place, they also become increasingly central players in protection – and, by extension, in policing. The role of private actors in policing and protection may vary – from informal partners in policing unplanned urban neighbourhoods, to private security firms, to the role of internet service providers in policing hate speech to the role of corporations in protecting food and pharmaceutical supply-chains from tampering. Social changes to 2050 may also lead to changes in emphasis in protection: where, today, significant law enforcement resources are devoted to enforcing narcotic control laws, by 2050 this may have been replaced by policing and protection of scarce natural resources or policing of cyberspace. The site and nature of law enforcement may, therefore, change significantly.

Increasingly, questions of ‘safety’ and ‘protection’ will involve provision of trust services and effective quality control in digitized business processes and cyberspace, rather than physical protection or real property integrity. Faced with the increasing prevalence of counterfeit goods, the growth in cybercrime, or the rising importance of intellectual property crimes, law enforcement may increasingly serve as arbiters or protectors in supply chains or in cyberspace. Police forces will also likely increasingly share this role with private actors. Today, for example, corporations, governments, and individuals hire private cybersecurity firms for the analysis, prevention, and investigation of cybercrimes, functions that, in other crime areas, have traditionally been the primary domain of law enforcement.

Global coordination will become increasingly central to the ability of individual states to police effectively. Investigating and responding to the recent WannaCry ransomware attack, for example, which affected computers in 153 different countries, has required dozens of different law enforcement agencies, as well as private companies such as Microsoft. The globalized nature of supply-chains and financial networks also means that coordination between public and private actors,
across borders and continents, is increasingly central to effective regulation and policing in those contexts. Digitization will also facilitate the distribution of criminal organization across jurisdictions in ways that fundamentally challenge territorially-based policing arrangements: a criminal group based in one country, for example, may eventually be able to share, through secure cybernetworks, a blueprint for a specific type of synthetic drug to consumers in dozens of countries, who can then print the drug on 3D printers for personal consumption or local distribution. This de-territorialization presents both challenges and opportunities for law enforcement.

Yet some themes and policing problems – such as border control – are likely to remain a constant. Control of violence will also likely remain a central focus, though here, too, there may be changes, as the use of big data and pervasive surveillance capabilities facilitate improved effectiveness in crime prevention techniques. Policing models such as focused deterrence or public health approaches to violence, which rely on highly targeted and coordinated law enforcement initiatives to isolate and prevent specific criminal behaviour, have been used to successfully reduce criminal violence in some cities across the United States, and may increasingly be used internationally. And, fundamentally, as we discussed earlier, the role that violence plays in organized crime will depend in significant part on policy choices by states, including how they choose to relate to organized crime.

A diversifying market for protection

By 2050, the suppliers operating in the market for protection will be increasingly heterogeneous. Preserving the safety and security of citizens will likely no longer be the sole preserve of the state: instead, protection will be supplied by different actors for different groups – and, potentially, using different normative systems as legitimating frameworks. States, municipalities and private actors may adopt new forms of insurance and risk-sharing to provide protection in new spaces, markets and value chains.

Private actors are increasingly significant as suppliers of physical protection services, both for private clients and for the general public. The transnational security industry, made up of firms who provide a range of services from travel security and kidnapping protection to business intelligence and fraud prevention, will also likely continue to grow. These companies are increasingly used by public and private sector clientele. A 2010 Washington Post investigation, for example, found a total of 1,931 private companies working on programmes related to counterterrorism, homeland security, and intelligence in the United States. And while little data exists on the size and scope of transnational security providers in the private sector, companies such as Control Risks and Kroll now employ thousands of people across dozens of offices around the world. Capacities that were previously confined to law enforcement will be more readily available for hire, and a growing number of private sector actors will develop in-house intelligence, security, and investigative units, as banks, insurance companies, and other sectors have today.

This trend is already visible: in the United States, Australia, and Israel, for example, private security personnel outnumber public police – sometimes, as in Israel, by as much as 3:1. In Europe, estimated rates of private security personnel are only slightly below public police rates. And the trend is not confined solely to high-income countries: Figure 11 (overleaf) shows the prevalence of police, armed forces, and private security in different regions.

Figure 10. Police, Armed Forces, and Private Security by Region and Government Type

<table>
<thead>
<tr>
<th>Region</th>
<th>Police</th>
<th>Private Security</th>
<th>Armed Forces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-Saharan Africa</td>
<td>268</td>
<td>112</td>
<td>207</td>
</tr>
<tr>
<td>North America</td>
<td>205</td>
<td>318</td>
<td>635</td>
</tr>
<tr>
<td>South America</td>
<td>138</td>
<td>190</td>
<td>347</td>
</tr>
<tr>
<td>South Asia</td>
<td>266</td>
<td>329</td>
<td>304</td>
</tr>
<tr>
<td>Europe</td>
<td>339</td>
<td>559</td>
<td>708</td>
</tr>
<tr>
<td>Central America and Caribbean</td>
<td>315</td>
<td>174</td>
<td>389</td>
</tr>
<tr>
<td>Russia and Eurasia</td>
<td>371</td>
<td>438</td>
<td>320</td>
</tr>
<tr>
<td>Asia/Pacific</td>
<td>206</td>
<td>552</td>
<td>707</td>
</tr>
<tr>
<td>Middle East and North Africa</td>
<td>250</td>
<td>851</td>
<td>354</td>
</tr>
</tbody>
</table>


This shift will present both opportunities and challenges. On the most basic level, this heterogeneity provides a larger pool of law enforcement resources – in some countries, for instance, private protection has helped to fill gaps created by government austerity. Investigations in some emerging crime areas, such as cybercrime, will require highly specialized expertise. Law enforcement authorities may increasingly choose to outsource certain capabilities to specialized firms or individual experts, rather than developing expertise in-house. Private security actors also play a significant role in protecting public infrastructure, which is likely to be increasingly critical as the digitization of infrastructure makes it more vulnerable to cyberattack.
Yet the growing heterogeneity of protection providers will likely also present significant governance challenges. Different actors have different interests, incentives, and economic motivations – and are responsible for the protection of different sets of actors and communities. These interests and allegiances may, at times, put them at odds with the interests or priorities of the state or of the broader communities in which they work, and may also lead to a lack of accountability. Public police often leave to work in the private sector, taking knowledge about and experience in proprietary law enforcement techniques with them and possibly diminishing the strategic advantage of the state. And there are a multitude of questions related to the training and regulation of private security forces, especially those operating across national borders, including what standards govern the nature of their work and what norms govern the use of force by these actors.

Technology, surveillance, and cyberpower

Technology and cyberspace, in particular, are already changing the nature of policing, and will continue to have a dramatic effect on both the concept and practice of protection through 2050.

As more and more human activity is captured in the form of digitally-stored data, intelligent automation, machine learning and other forms of predictive analytics will become an increasingly critical component of law enforcement. Police forces will likely increasingly focus on ‘intelligence-led policing models’, using data to guide operational and tactical decisions. This includes the use of ‘predictive policing’ – using artificial intelligence or machine learning to detect patterns of criminal behaviour, and thus predict future outbreaks. Many of the tactics that underpin predictive policing are not new: police departments traditionally, for example, use crime-mapping techniques to identify hotspots and allocate resources. But increasingly, police departments use new technologies, as well as larger and more diverse data sets, to conduct analyses on both a much larger scale, and with more individual-level analysis. Here too, there will be increased opportunity for private actors in the business of protection: law enforcement will require the cooperation of private companies that control the gates to critical data and intelligence, communications and value-transfer platforms, and proprietary analytical tools and approaches. Already, we see some important firms emerging in this role.

Law enforcement’s increased reliance on technology may raise questions about the right to privacy and the potential for racial bias or selective targeting. Yet technology will likely create many opportunities for law enforcement, allowing police forces to enhance intelligence collection, increase efficiency, and adapt to changing criminal tradecraft. While law enforcement may in some ways struggle to stay ahead of advances in encryption and anonymous digital marketplaces, it will also adapt, using more sophisticated detection techniques. Although virtual currencies, for example, are criticized for the anonymity they offer those engaged in crime or illicit transactions, their rise may actually reduce the incidence of fraud and/or make it easier for law enforcement to track the flow of illicit online payment – as opposed to cash hidden in a shipping container.

In addition, technology may improve police-community relationships and lead to increased transparency. Developments in information and communications technology, for example, have opened new avenues for citizen-police communication and crowd-sourcing of critical intelligence. In many parts of the world, high levels of corruption and crime have led to diminishing public trust in the police. Increased transparency stemming from crowd-sourcing or publically available crime maps may help to improve community-police relationships and transparency. And in countries where government and law enforcement lack legitimacy, such technologies may also be used by populations as an alternative method to advance security and hold police accountable. Blockchain, the distributed ledger technology that underpins Bitcoin, for example, may be used to increase transparency and reduce fraud in everything from public databases (such as land registries) to registers of the ownership of luxury goods or works of art.
Conclusion: Strategic Policy Implications

Several key themes emerge from within this analysis regarding the changing nature and location of criminal rents – and the governmental power that some organizations will derive from controlling them. Organized crime and corruption will continue to be present in our lives in 2050, interwoven with and through the systems of governance, whatever they look like. But the policy choices states make in the next few years may determine whether organized crime is fused with the power of the state and other actors with significant governmental power, bending institutions away from the values of universal human rights, accountable democracy and state responsibility; or whether organized crime’s power remains marginalized from the state and from global governance.

Cyberpower and the nation-state

One key theme arises from digitization and the rise of cyberpower. The control of territory and subjugation of populations within them (‘biopower’), which has been at the heart of the modern state’s governmental power, is increasingly being supplemented by ‘cyberpower’ – the ability to control digital data and flows and regulate cyberspace. States already face important policy choices here. Will they cooperate to collectively protect cyberspace, as it is now, as largely a space for private activity, innovation and organization? If so, who will provide protection within that space – protection from extortion, theft, fraud and coercion, protection of human rights such as privacy, freedom of speech and association, and family life? Will states be comfortable with corporate actors taking on these protective – and policing – functions by default? Or will some states seek to impose a more Westphalian vision on cyberspace?

The emergence of digital value chains (facilitated by additive manufacturing, AI and the Internet of Things), together with virtual currencies (VCs) and peer-to-peer payment systems, extends these questions even further, as it may pose acute challenges for state control of economic value. As non-state value transfer systems become more extensive, we may see communities or municipalities banding together – or even cooperating with commercial partners – to create autonomous economic archipelagos stretching across national borders, within which protection and trust services are provided to a closed off but dispersed network.293 As we explain further in the boxes below, in a benevolent model, this might be thought of as an extension of the networks of city states such as the Hanseatic League that competed, for a time, with the modern nation-state as the primary provider of governance in Western Europe.294 A less rosy view, however, would suggest that these archipelagos risk extending the ‘off-shore’ model we see emerging currently, which allows the rich and powerful – and the criminal – to escape effective governance and regulation.

The danger is of the emergence of a highly ‘crooked’ system of governance that serves the interest of transnational kleptocratic networks and a highly mobile, secure ‘1 per cent’ elite – while growing portions of world population are vulnerable to significant environmental, labour market and health insecurity.

What is the ‘public interest’ in a privately governed world?

That possibility points to a second key theme: the increasing importance of private actors in governance – from the provision of neighbourhood policing services in favelas to the provision of trust services in global value chains, verifying the security of online transactions and guaranteeing the safety of foodstuffs. States will increasingly have to partner with non-state actors to govern. It is no accident that in a recent, much-noted op-ed, the current US National Security Adviser H.R. McMaster argued that ‘the world is not a “global community” but an arena where nations, nongovernmental actors and business engage and compete for advantage’ (emphasis added).295

This brings major operational challenges; but perhaps even more profound – and less remarked – strategic and governance challenges. If corruption is, as we set out at the beginning of this report, the abuse of a position of public trust for private gain, and private actors are increasingly empowered to take on public governance functions, the risks of abuse of public power for private gain would seem naturally to rise. Corruption risks becoming, as Sarah Chayes has put it, ‘the operating system’.296 In some ways, this reflects the way governance has ‘worked’ for some time, with formal institutions of accountability and institutions shot through with informal patronage systems and social networks protecting communities (tribes, families, other social groups, even mafias) other than the national ‘public’. The de-territorializing impacts of digitization (discussed above) may exacerbate this problem further.

Yet the deeper challenge is even more profound. As private interests take on greater governmental roles, the very concept of ‘the public’ will become blurry. The first few words in the quote from McMaster above, bear close attention – ‘the world is not a “global community”...‘. McMaster has faith in nations as imagined communities and the primary source of governmental power, but little time for the notion of a universal community or, apparently, universal public values. Yet the increasing role of non-state actors in governance opens up the very real possibility that individuals will increasingly owe their allegiance not to nations, but to communities otherwise imagined – to the umma or the caliphate, to maras and mafias, or to new identity communities.

New types of community may ‘govern’ individuals’ conduct, posing challenges for how we understand the very notions of the ‘public’ and the ‘public interest’, and the ‘public policy’ goals towards which strategic action should be aimed. And organized crime and corruption, as strategies for developing
socio-economic power, may be central to some of these new forms of governmentality.

**Investing in global commons and a rules-based international order**

This poses significant challenges for states that believe in a rules-based international order based on universal human rights. The central challenge is to determine what steps need to be taken now in order to minimize the potential governmental power of organized crime and corruption in 2050.

As we have seen through this analysis, this requires careful reflection on how policy choices will shape opportunities for the organized extraction of criminal rents, and in particular attention to the location of vulnerability (and hence the demand for protection), and of gates between different jurisdictions and realms (creating arbitrage opportunities).

A common theme that seems to emerge is the central importance in investing in the protection of well-governed global commons, because they minimize the opportunities for rent extraction. By 2050 this might involve, for example, strengthened governance to ensure a rules-based, safe, and accessible internet; stronger collective governance of the climate, to ensure safe, reliable and neutral access to ecosystem services and essential resource flows; and new forms of governance to ensure macroeconomic stability following the move away from fiat currencies to distributed ledgers, peer-to-peer payments and other non-state value transfer systems.

This suggests two major changes in global governance. First, a rapid and clearer move from inter-governmental to multi-stakeholder governance arrangements, using the leverage of non-state actors to deliver public goods. Second, stronger systems for collective investment in prevention, reduced vulnerabilities and resilience. Policies and institutions that provide broad-based protection against vulnerabilities arising from climate change, continuing large-scale migration, workplace automation, artificial intelligence, and other frontier technologies will not only create resilience, but thereby reduce the opportunities for criminal and pernicious actors to occupy the protection spaces left vacant by states.

**Three scenarios for governance in 2050**

By 2050, technological, physical and social changes will have generated a variety of new ‘spaces’ and contexts over which states exercise only limited control and governmental power. New forms of vulnerability will drive new demands for protection. Individuals and communities will seek insurance and security in the face of labour market disruptions, environmental stress, unplanned urbanization, and cyber-vulnerability. States will have to work with a variety of other actors to protect people in these contexts, and to ensure that the limits of state governance do not lead to other, more crooked, providers of governance emerging in those spaces.

What form will these new systems of protection take? And how will they operate across the different markets and contexts discussed in the seven sections above? Drawing on the thematic insights above, in the boxes below we outline three possible scenarios. These are not intended to be predictive; rather, they are intended as schematic illustrations of some of the ways in which both state and criminal governance may evolve – and interact – by 2050.

### Scenarios

**Hobbes**

In this scenario, large swaths of the population do not receive – or expect – to be protected by states. Corruption, privatization, and government austerity have bent public institutions away from their original purpose, and while the Westphalian system continues to exist in name, the social contract has been largely eroded. Faith in democracy has corroded considerably, as many people see democratic institutions as providing a thin veneer of legitimacy for predatory elites. Those elites have become hard to distinguish, in many peoples’ minds, from transnational criminal organizations. Public military and law enforcement systems have been severely curtailed or corrupted; instead, security and protection are reserved for those who can pay for it. Private security forces protect individual neighbourhoods and communities, and corporate actors protect privately controlled value chains and business processes.

Among the rest of the population, unemployment, environmental shocks, and rapid urbanization have left entire communities unprotected and unserved by effective state governance. In the absence of state-sponsored resource-sharing agreements, there is increasing competition for scarce resources, including food, water, and land, with local urban warlords and mafias serving as informal protectors and governors. With much commerce now conducted through cyber-enabled machines and networks, supply-chain integrity – from food to pharmaceuticals – is severely compromised. Cheaper, more insecure markets are increasingly flooded with counterfeit food, medicines,
and other goods, while those who can afford to pay a premium for luxury goods known to be associated with quality and security.

In this world, cyberspace is a hodge-podge of carefully regulated and wild-west networks and systems, within which the security dilemma is pervasive. With digital data critical to every component of everyday life, attacks on individuals, corporations, and state institutions are common – but divergent cybercrime models have emerged. Low-level cyber-criminality – petty theft, fraud, and hacking – provide one of the few forms of economic opportunity for low-income individuals, and end users become accustomed to high levels of insecurity and uncertainty in their online lives. Simultaneously, state and private elites contract sophisticated transnational cybersecurity providers to provide both defensive and offensive capabilities.

Disillusioned with and underserved by the state, poorer local populations look elsewhere for protection, meaning, and identity. New identity communities – from local gangs to diaspora communities to transnational religious groups – emerge as providers of protection and services, creating new, hyper-local and community-based forms of economic exchange and trust services. These groups increasingly govern the behaviour of their members, dictating norms around the use of force and the allocation of resources – both in the physical world and in cyberspace. In many cases, the services and security provided to their members may be more robust than the protection provided by the state. But in some cases, unimpeded by state regulation or oversight, such groups may also extract significant criminal rents in the process.

**Hanseatics of the 21st Century**

In this world, states, municipalities and corporations band together to create closed governmental archipelagos straddling physical space and cyberspace. These modern-day 'Hanseatic Leagues' offer safe trading spaces, each with its own virtual currency, digital commerce platform and 'internet'. They provide significant scale for multiple communities to pool risk and access resources to address shared vulnerabilities against risks ranging from extreme weather events to pandemics to cyberthreats. Each 'league' protects the economic, social, and political interests of its members, while facilitating free trade within and between partners.

Whereas Westphalian nation-states tended to bind contiguous and adjacent urban and rural communities together through a shared national narrative, the new Hanseatic model sees many megacities forming strategic alliances not with adjacent rural areas, but with far-off resource-rich zones. In these leagues, megacities provide financial and physical and cybersecurity, while resource-rich rural areas provide resource security.

Legitimacy is conferred by results – creating strong incentives for leagues to compete with each other for access to resources and populations. Gatekeepers controlling that access may be in a strong position to extract criminal rents. Criminal norms and law enforcement are highly politicized. Some communities operating outside 'league' structures are treated as 'outlaws', and are forced into predation as a survival strategy. At the same time, some parasitic non-state actors are tolerated as informal auxiliaries and proxies for league actors, extending their control into and over criminal markets and hard-to-reach populations. (For those leagues that rely on democratic elections, these groups also play an important role in accessing and mobilizing voting blocs in under-served communities.) In exchange for buy-in from corporate and political elites – and to maintain a competitive advantage – some leagues turn a blind eye to corruption and laundering of criminal rents.

**Heterogeneity**

In the final scenario, state-based governance has adapted, creating new partnerships to manage new risks presented by environmental, economic, and technological changes. Recognizing that changes in cyberspace, in financial systems, and in the environment challenged concepts of state sovereignty, states have instead chosen to partner with private corporations, international organizations, and each other to find new insurance-based social protection and other risk-mitigating solutions. This has resulted in a system of heterogeneous but networked governance, in which public actors work together to establish and maintain the incentive structures and accountability systems that motivate private actors to help protect public goods, from cyberspace to coral reefs. By addressing these protection needs, the potential for organized criminal growth has been reduced. At the same time, the combination of public and private interests to govern everything from payment systems to analysis of megadata to protection of scarce resources has created significant possibilities for corruption.

In cyberspace, for example, an international group, composed of both states and key cyberinfrastructure providers, operate under a multistakeholder agreement governing cyberspace as a global commons, and assuring universal access, net neutrality, demilitarization and protection of human rights. A heterogeneous governance arrangement has also emerged governing access to proprietary artificial intelligence and machine learning technologies, virtual reality and virtual currency technologies – all of which have become central to participation in global value-chains. Groups of states have entered bilateral agreements with the corporations that
own the key technologies, exchanging access to the infrastructure for access to their populations and markets, based on corporations’ acceptance of a variety of financial, social, labour and human rights responsibilities. Technology companies have taken on responsibility for ensuring supply chain integrity, using blockchain and other technologies. And some states, supported by multilateral organizations, have invested in global R&D processes to develop new technologies to fight climate change.

At the heart of this scenario is a recognition that many of the vulnerabilities that people face – and that pose a significant risk to states’ hold on governance – can only be effectively addressed through international and multistakeholder cooperation. Protection is approached not as a zero-sum game, but as a cooperation game, requiring sharing of risk and pooling of resources. The resulting public solutions are – like the state itself – vulnerable to corruption and manipulation. But they offer some hope of protection of public interests, without which, private – and often crooked – actors will emerge as the primary providers of protection and governance.

ENDNOTES


4 Ibid.


10 The definition of serious and organized crime adopted by the UK government, for example, includes some organized criminal activity that operates on a non-commercial basis, such as organized paedophilia. See “Serious and Organised Crime Strategy” (HM Government, October 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf. In this report, we deliberately focus on organized, rather than ‘serious’ crime.


14 Cockayne, Hidden Power.

15 Chayes, Thieves of State.

16 We are indebted to Nils Gilman for the discussions that helped shape this point.


21 We are indebted to Colin P. Clarke, Phil Williams, and Steven Davenport for this framing.

22 “World Population Prospects: The 2015 Revision, Key Findings and
57 See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000? Because Vietnam Thinks It Cures Cancer and Hangovers.”

58 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

59 Ibid.

60 Ibid.

61 See, for example, Guifford, “Why Does a Rhino Horn Cost $300,000? Because Vietnam Thinks It Cures Cancer and Hangovers.”

62 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

63 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

64 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

65 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

66 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

67 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

68 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

69 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”

70 Source in part to a single rumour that rhino horn cured a local politician of cancer. However, other dynamics appear to have been more influential. See, for example, Guilford, “Why Does a Rhino Horn Cost $300,000?”
Crooked States

81 See for example the allegations around some Eastern European entities such as TIM of Bulgaria: see e.g. Jan Puhl, “Bulgarien – In Flammen,” *Der Spiegel*, no. 19, 2013, 86-88.
84 You’re Eating and What You Can Do about It, *Food First* (Algonquin Books, 2016).
86 See also for example the allegations around some Eastern European entities such as TIM of Bulgaria: see e.g. Jan Puhl, “Bulgarien – In Flammen,” *Der Spiegel*, no. 19, 2013, 86-88.
89 United Nations and Department of Economic and Social Affairs, *World Urbanization Prospects, the 2014 Revision: Highlights, 2014*.
90 According to the UN Department of Economic and Social Affairs, “a majority of city dwellers [today] live in cities that face high risk of disaster-related mortality or economic losses.” See UNDESA, “The World’s Cities.”
94 Muggah, “Urban Governance in Fragile Cities.”
97 John de Boer, Robert Muggah, and Ronak Patel, “Conceptualizing...
City Fragility and Resilience.”


128 Muggah, “Urban Governance in Fragile Cities.”


130 Enrique Desmond Arias, Criminal Enterprises and Governance in Latin America and the Caribbean, 1 edition (New York, NY: Cambridge University Press, 2017); Cockayne, Hidden Power.


135 Colin P. Clarke, Phil Williams, and Steven Davenport, “The Future of Transnational Organized Crime” (On file with the authors, 2017).


137 Cockayne, Hidden Power; Andreas and Wallman, “Illicit Markets and Violence.”


140 Andreas and Wallman, “Illicit Markets and Violence.”

141 Ibid.


144 Ibid.

145 Cockayne, Hidden Power.

146 Smith, et al., No One Has Ever.


148 Ibid.

149 Ibid.


152 Ibid.

153 Ibid.


155 European Monitoring Centre for Drugs and Drug Addiction, “New Psychoactive Substances in Europe: An Update from the EU Early Warning System.”


163 Ibid, 11.


165 Ibid.

166 Ibid.

167 Jane Maunteney et al., “The Internet and Drug Markets: Summary of Results from an EMCDDA Trendspotter Study” (Lisbon: European Monitoring Centre for Drugs and Drug Addiction, January 2015). Alexandra Hall paper


169 Ibid.


162 James Cockayne and Summer Walker, “What Comes After the War on Drugs?”, Sheldon X. Zhang and Ko-in Chin, “A People’s War: China’s Struggle to Contain Its Illicit Drug Problem”.

163 James Cockayne and Summer Walker, “What Comes After the War on Drugs.”

164 Ibid.


167 UK Ministry of Defence, “Global Strategic Trends - Out to 2045,” 57.


169 UK Ministry of Defence, “Global Strategic Trends - Out to 2045,” 57.


181 Ibid.


190 See for example Brian Fung and Andrea Peterson, “America uses stealthy submarines to hack other countries’ systems”, The Washington Post, 29 July 2016.
See “Egypt catches divers cutting Internet cable amid disruptions”, Reuters, 27 May 2013.


Ives and Mozur, “Small Countries’ New Weapon Against Goliaths.”

Clarke, Williams, and Davenport, “The Future of Transnational Organized Crime.”


We are grateful to Douglas Taylor for the discussion that helped shape this point.


Cockayne, Hidden Power, 114.


Corkery and Goldstein, “North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist.”

Cockayne, Hidden Power, 224-226.


Ibid.


Kar and Spanjers, “Illicit Financial Flows to and from Developing Countries. 2005-2014.”


Available at Kar and Spanjers, “Illicit Financial Flows to and from Developing Countries. 2005-2014.”


Offshore_Revisited_120722.pdf.


220 Dong He et al., “Virtual Currencies and Beyond: Initial Considerations,” IMF Staff Discussion Note (International Monetary Fund, January 2016).

221 Ibid.


226 Dong He et al., “Virtual Currencies and Beyond: Initial Considerations.”

227 Ibid.


229 Ibid.

230 Dong He et al., “Virtual Currencies and Beyond: Initial Considerations.”

231 Ibid.

232 Ibid.

233 FATF, “Virtual Currencies: Key Definitions and Potential AML/CFT Risks.”


235 Dong He et al., “Virtual Currencies and Beyond: Initial Considerations,” 34.

236 Ibid; FATF, “Virtual Currencies: Key Definitions and Potential AML/CFT Risks.”

237 Dong He et al., “Virtual Currencies and Beyond: Initial Considerations,” 34.

238 FATF, “Virtual Currencies: Key Definitions and Potential AML/CFT Risks.”


243 Carothers and Youngs, “The Complexities of Global Protests.”

244 Ibid.


247 The six countries surveyed were Spain, Brazil, India, South Africa, the United Kingdom, and the United States. See “Working for the Few: Political Capture and Economic Inequality.”

248 Carothers and Youngs, “The Complexities of Global Protests.”


251 Andy Wynne, “Inequality Causes Corruption”


255 Finn Heinrich, “Corruption and Inequality.”


257 Anderson and Page, “Weaponising Transparency.”

258 Cockayne, Hidden Power.

Chayes, “Corruption and State Fragility.”


Cockayne, Hidden Power.

“Corruption: The Unrecognized Threat to International Security.”


“Corruption: The Unrecognized Threat to International Security.”


Willis, “WannaCry.”


Available at http://wispindex.org/sites/default/files/downloadables/WISP%20Report_EN_WEB_0.pdf.


Ibid.

Ibid.


Slansky, “The Persistent Pull of Police Professionalism.”


“Accenture Public Safety Technology Vision 2016.”


Ibid.