UNITED NATIONS UNIVERSITY

United Nations University
Research Brief
October 2017

Preventing the Rise of Crooked States:

How can development and stabilization policies prevent the criminalization of governance?

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

This research has been funded by UK aid from the UK government; however, the views expressed do not necessarily reflect the UK government's official policies.

ISBN 978-92-808-9059-4

Table of Contents

Executive Summary

In the coming decades, a wide array of socioeconomic, environmental and technological changes will create new challenges for developing states. Climate change, the automation of work, cyber-threats, unsafe supply-chains and unregulated financial systems will create new risks and vulnerabilities. States may increasingly struggle to provide protection and services in new and emerging spaces – including cyberspace, emerging financial systems and unplanned urban spaces vulnerable to shocks from climate change.

Without the protection of the state in these spaces, people will look elsewhere. In some cases, businesses, private actors or civil society will emerge to address risk and provide insurance against insecurity. But in others, criminal actors will step in – providing not just protection and services, but also dictating norms and offering meaning and identity to citizens. They may corrupt formal and legitimate institutions, businesses and markets, bending them away from their stated purpose. The result may be a significantly expanded role for organized crime in governance in the next three decades – and the rise of 'crooked states' and crooked governance more broadly.

Drawing on a larger study on the future of organized crime and corruption out to 2050, this policy brief looks at how the changing nature of organized crime and corruption may impact state fragility, inequality and conflict in the coming decades. It examines three areas where tomorrow's vulnerabilities may create opportunities for new forms of criminal governance, and considers how development and stabilization policies can encourage resilience in the face of these criminalizing tendencies – and prevent the rise of crooked states in the first place.

Vulnerabilities, protection and resilience

The first section of the brief considers how an array of stressors – including climate change and resource insecurity, unplanned urbanization and labour market disruptions – may challenge state governance in the coming decades. Struggling to keep up with environmental, demographic and technological changes, state institutions in developing countries may lack the resources or the legitimacy to meet the protection needs of their residents. And in some states, high levels of corruption and illicit financial flows may further undermine state capacity and authority. Instead, criminal and corrupt actors may be well-positioned to fill these needs – and to develop an expanded role in governance.

Preventing and reducing the role of criminal groups in governance will require development policies that help states, working with civil society and legitimate businesses, provide protection and reduce vulnerabilities. Key policy implications include:

- **Using social protection policies to address vulnerabilities** and reduce demand for criminal protection. This may include economic livelihood programming, interventions designed to ensure the equitable distribution of resources, and investment in social service provision or infrastructure development.
- **Minimizing the demand for criminal protection created by shifts in the labour market**, through programming that encourages economic resilience, job training initiatives and alternative forms of livelihood provision.
- **Exploring how anti-corruption interventions can be used to protect state institutions against organized crime**, for example through strategic interventions to address the links between corruption and political finance and working out which interventions shift social norms to promote resilience to organized crime.
- **Strengthening the counter-organized crime role played by global finance in development outcomes**, improving financial transparency and global coordination to reduce opportunities for corruption and illicit financial flows.

Stabilization and peacebuilding

There is increasing recognition that organized crime and illicit economies play a significant role in conflict-affected settings, and may impede stabilization and peacebuilding efforts. The second section of the brief considers the ways in which conflict creates entry points for organized crime and corruption, and how organized crime impacts post-conflict transitions. During and after conflict, norms around illicit activity, criminal-political collaboration, and the use of violence may be eroded, presenting opportunities for organized crime. Criminal groups may subvert post-conflict transitions, exercising political power and undermining the long-term legitimacy of state institutions.

Diminishing the economic and governmental power of criminal groups in post-conflict settings requires careful management of transition dynamics and political settlements. Key policy implications include:

- **Crime-proofing stabilization efforts** to ensure that interventions do not inadvertently contribute to criminal networks and illicit flows, and do not reinforce or legitimize criminal behaviour or criminal-political collusion.
- **Strategically engaging groups with criminal agendas** in peace processes, when and where such groups exercise significant political power and otherwise risk becoming spoilers. This may include incentives and inducements designed to motivate such groups to abandon undesirable behaviour.
- **Building effective governance, not just government.** This requires looking beyond state governance institutions, harnessing the social and political power of non-state actors during transition periods and promoting 'bottom-up' forms of governance and protection.

Cyber-development and cyber-inequality

As cyberspace becomes increasingly central to every aspect

of social and political life, digitization is leading to a reorganization of geo-economic power and disrupting global value chains. These shifts have significant implications for the future of organized crime and corruption – and increasingly, they will also challenge our understanding of security, social inclusion and state-citizen relationships. The third section of the brief considers how development policies may need to account for the risks that changes in cyberspace could lead to crooked governance, if not addressed.

Promoting resilience and security in cyberspace requires consideration of where new vulnerabilities will arise and how these vulnerabilities may generate demands for cyberprotection. Key policy implications include:

- Bolstering cyber defences in developing states to ensure that governments can prevent against and respond to cybercriminality. This may include development assistance that helps to secure critical infrastructure, improve cyber-hygiene and expand the cyber capacity of state security institutions.
- Leveraging technology to improve development outcomes, helping developing states harness the positive impacts of digitization and cyberspace to promote good governance and foster economic and social resilience.
- Considering global cyber-governance to ensure a rules-based, safe and accessible internet. Development actors should begin to consider how policies such as net neutrality, universal access, and data protection might impact future development trajectories and prevent against the emergence of new forms of cyber vulnerability and exclusion.

In each of these areas, limiting the long-term criminalization of governance will require short-term policies focused on prevention. It will require careful consideration of where new vulnerabilities – and new demands for protection – will arise, and whether criminal actors may step in to provide that protection. Development and stabilization policies should aim to foster resilient, effective and legitimate governance structures, to crowd out criminal governance and protect legitimate governance going crooked.

This will require thinking beyond state-based governance structures. Increasingly, states will need to work with other actors – including businesses, civil society and legitimate non-state actors – to manage new challenges and provide new forms of protection. There will also be an increased need for multi-stakeholder initiatives at the global level. Policies and institutions that provide broad-based protection against vulnerabilities arising from climate change, labour force disruption, conflict and cybercrime will not only create resilience, but will also reduce opportunities for criminal and pernicious actors to occupy the protection spaces left vacant by states. Smart development policies and practices will, in other words, help prevent the rise of crooked states and governance structures in the first place.

Introduction

Every five years, the UK Ministry of Defence undertakes a whole-of-government strategic trends analysis process, seeking to understand the long-term strategic outlook for UK defence and security. The 6th edition of the report, *Global Strategic Trends: Out to 2050*, will, for the first time, include a stand-alone chapter on organized crime and corruption. UN University (UNU) was commissioned, through the UK Department for International Development (DFID), to develop this analysis, exploring how organized crime and corruption may evolve over the next three decades. UNU was asked in particular to consider how the changing nature of organized crime and corruption may relate to state fragility, inequality and conflict.

Our report for that process, entitled '*Crooked States*', predicts a significantly expanded role for organized crime in governance over the next three decades. The reason for this is simple. Climate change, the automation of work, cyber-threats, unsafe supply-chains and unregulated financial systems will create new risks and vulnerabilities. States are struggling to govern a variety of new spaces that are emerging – including cyberspace, distributed financial systems such as Bitcoin and Ethereum, and unplanned urban spaces vulnerable to shocks from climate change. Without the protection of the state in those spaces, people will look elsewhere.

Whoever protects people from those risks will win their loyalty. In some of those spaces, legitimate business may provide that protection. In others, organized crime will be well poised to provide that protection, and to use the resulting loyalty to govern. The power that organized crime wields in those spaces makes it an ally for unscrupulous political actors – and in return, gives it influence over those actors. The result may be a movement from fragile and failed states to crooked ones.

In some cases, states and criminal organizations may cooperate, or even collaborate, to maximize their governmental power, sometimes forming what Sarah Chayes describes as 'transnational kleptocratic networks'.[1] In other cases, they will compete directly. And in yet others, the state may largely abdicate its governmental responsibilities, leaving space for other governmental powers to emerge.

The way in which organized crime and corrupt actors exploit the structural changes in the years ahead will often depend on the choices and actions of states. Organized criminal groups are frequently viewed as infiltrating the state, using corruption and coercion to bend state institutions away from their true purpose. But in many cases, the state itself opens up space for criminal governance, either through its inability or unwillingness to govern certain spaces, neighbourhoods, or markets, or through active complicity with organized criminal groups.[2] States must also recognize that they are sometimes competing directly with these groups. In

marginalized communities – from minority ethnic enclaves to isolated rural communities – criminal networks may enjoy more legitimacy with local populations than state institutions, precisely because they are less predatory and more reliable.[3]

Drawing on *Crooked States*, this policy brief looks at the near-term implications of this analysis for development and stabilization policies. We argue that limiting the long-term criminalization of governance requires policies focused on prevention in a wide array of policy areas, from the environment to cyberspace. We highlight various policy choices we believe will be critical to address and prevent the growth of criminal governance, and its associated negative effects.

The first section of the brief considers how new vulnerabilities may empower criminal actors, and how development policies can encourage resilience in the face of these criminalizing tendencies. A second section considers how stabilization efforts may need to account for the risk of organized crime and corruption. And a third section considers how changes in the role of cyberspace may impact development policies. In each section, we briefly consider the main shifts that will drive insecurity and present opportunities for organized crime, explaining what we do and do not know about the way in which these shifts will interact with development concerns, and offer a short assessment of policy implications and recommendations.

A note on key terms

Organized crime and corruption are both highly contested concepts.[4] *Crooked States* treats organized crime and corruption as distinct but related phenomena, both concerned with the extraction of *criminal rents*. 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).[5] Organized crime usually 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.[6]

Different types of actors play different roles in the production and extraction of these criminal rents. Protection theory, for example, draws a distinction between criminal 'entrepreneurs', or those who supply and move illicit goods in criminal markets – extracting rents from the sales of the goods and services themselves – and 'protectors' or 'violent entrepreneurs', who supply protection in these markets, extracting rents from that protection.[7] The demand for protection 'occurs when there is a lack of trust between the market participants, or where their interests are insufficiently safeguarded by legitimate actors and entities (typically the state)'.[8] Some actors, especially those providing protection, may develop the power to not only resolve disputes within the market, but, closely related, to set norms, providing the framework by which actors in that market or community regulate their own conduct. We describe this as 'governmental power'.[9]

Our inquiry is primarily concerned with this intersection between organized criminality and governance, rather than, for example, the economic dynamics of illicit markets. Corruption is a key method for exchange and interaction between formal governmental actors and these informal actors, exerting hidden power over formal politics. The entrenchment of this influence leads to what we describe as 'crooked states'.

(*For more details on our methodology, please refer to the companion report:* James Cockayne and Amanda Roth, Crooked States: *How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now* (UNU: New York, 2017).)

1. Vulnerabilities, protection and resilience

The negative effects of organized crime and corruption on development are increasingly recognized by both academics and policy-makers. Organized crime and corruption may undermine security, co-opt limited resources, and impede long-term stability and economic development.[10] However, the findings in Crooked States also push us to consider how development policy choices may themselves unwittingly create opportunities for organized crime, and open space for alternate providers of protection – or, alternatively, prevent the emergence of crooked governance.[11]

1.1 How changes to 2050 will facilitate organized crime and corruption

Crooked States highlights several areas where vulnerability may open up opportunities for rent extraction and the provision of protection – and, in turn, criminal governance.

Climate change and resource insecurity

Without rapid technological or policy advances in the coming decades, demographic and environmental changes may lead to growing resource insecurity in significant parts of the developing world by 2050. The UN estimates that half of the world's population will face water shortages by 2035, and that more than 30 countries (nearly half of them in the Middle East) will experience extremely high water stress.[12] Food scarcity, similarly, may be increasingly prevalent by 2050, as population increases and economic growth increase demand, while climate change, pollution, and a rise in conflict and natural disasters threaten supply.[13] While food production will increase, it may not be sufficient to meet demand – and increases in food production may not occur in the regions where additional food is needed most.[14]

Shortages of water, food, land, and other critical resources will create significant vulnerabilities for populations in developing countries. In some states, government-managed resource-

sharing arrangements or interventions by international actors may help to mitigate the effects of resource insecurity. But scarcity is likely to drive up the rents associated with the supply and distribution of resources, and criminal and corrupt actors are likely to take notice. These actors may seek to govern the supply and distribution of critical resources – and to offer citizens protection against uncertainty and risk where the state cannot. In many parts of the world, organized criminal groups already extract significant rents from the exploitation and trafficking of natural resources such as gold, diamonds, and timber.[15] As more everyday resources become scarcer, this criminality may extend to water, food or other critical items. In water-stressed cities such as New Delhi and Karachi, for example, local criminal networks are already involved in the illicit supply and distribution of water.[16]

Urbanization, demography and service provision

In some developing states, rapid urbanization, significant population increases, and the negative effects of climate change may significantly challenge social-service provision. Between now and 2050, urbanization will occur at a remarkable rate, especially in Africa and Asia.[17] The majority of 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.[18] This 'unplanned urbanization' may present significant challenges for governance and social structures, especially in littoral areas most vulnerable to the effects of climate change.[19] State institutions and municipal authorities in developing countries may lack the legitimacy or capacity to fulfil core functions for residents, including law enforcement, public infrastructure development, social service provision, and disaster recovery. Informal or parallel economies are also likely to develop, as and where the pace of urbanization eclipses the creation of job opportunities in the formal sector.[20]

In these spaces, criminal actors may step in to provide services and protection to residents, and to serve as intermediaries between the state and the population.[21] They may govern informal or parallel economies, regulate the allocation of scarce resources, and deliver services to communities neglected by state institutions. This allows criminal groups to cultivate social support and legitimacy, which may then provide cover for other illicit activities. In Mozambique, for example, criminal groups 'provide commodities or broker the provision of basic services' in regions where the state has little or no presence, allowing them to gain social and political credibility among local populations.[22] In Brazil's *favelas*, organized crime groups provide protection against violence and insecurity, regulating certain forms of criminality and arbitrating disputes.[23]

Labour market disruptions

Technological changes may threaten livelihoods and increase economic insecurity in some developing states. By 2050, technological advancements and developments in machine learning, artificial intelligence, and automation may lead to job loss in a wide range of sectors. In April 2017, World Bank President Jim Kim warned that two-thirds of jobs in developing countries could be lost to automation in the coming years, leading to increased conflict and migration flows.[24] While job loss due to automation has been a concern in high-income countries for some time, a recent study found that in countries as diverse as Nigeria, Ethiopia, India, Argentina and Thailand, anywhere from 65 to 85 per cent of jobs may be vulnerable to automation.[25] Some of these states, such as Nigeria, Ethiopia and India, are also likely to experience rapid population growth and urbanization in the coming decades.[26] The combination of these trends may leave large numbers of people – especially young people – searching for livelihoods and coping and survival strategies. Tax revenues in some developing states may be further impacted by these labour market disruptions, which may increase unemployment and economic insecurity. While wealthy states may be able to invest in new industries or provide new forms of social welfare to minimize these disruptions, smaller, low-income states will likely struggle to adjust.[27]

In such places, criminal livelihoods may become more appealing. Development actors increasingly recognize the role that criminal groups and networks play in offering livelihood options – as well as meaning and identity – to individuals who have limited options and little economic or social support from the state.[28] Already, in some regions, where employment opportunities are limited and there is little effective government provision of social services and support, organized crime provides one of the 'very few available ladders of economic mobility and social advancement'.[29] In states where job loss is widespread and states are ill-equipped to respond, participation in organized crime may significantly increase.

Illicit financial flows and the digital economy

Changes in the digital economy may present new opportunities for criminal and corrupt actors to disguise or launder the proceeds of illicit activity – and may further impede development trajectories. Illicit financial flows already have a significant negative economic impact in developing countries, reducing tax revenue, economic production and private investment. They damage state institutions by weakening the role of government, undermining government accountability and tax regimes, and catalysing illegal activities.[30] And illicit flows are 'intimately linked to large-scale corruption', meaning that efforts to tackle corruption and poor governance will also require policies designed to stem illicit flows.[31]

Multiple dynamics have contributed to the increase in illicit financial flows in recent decades. Regulatory policy choices and governance arrangements – especially relating to resource governance, bank secrecy, non-disclosure of beneficial ownership, and tax haven arrangements – have made it easier to quickly and easily obscure the providence of criminal

rents.[32] Some of these policies are, in turn, the product of emphasis on capital mobility and financial globalization over the last three decades.[33] This has been further compounded by the digitization of finance, which has helped to facilitate illicit financial flows and made it easier to earn and launder money illegally.[34] Online banking also allows individuals to quickly and easily transfer money, maintain offshore banking and investment accounts, and set up (or liquidate) shell companies.[35]

In the coming decades, the rise in virtual currencies, particularly distributed ledger technology based currencies such as Bitcoin and Ethereum, may further compound these challenges. Virtual currencies – 'private sector systems that, in many cases, facilitate peer-to-peer exchange bypassing traditional central clearinghouses'[36] – will likely increasingly compete with cash and fiat currencies for a share of the global economy. Often anonymous by design, such currencies allow for rapid and easy cross-border payments over the internet or by mobile phone. Individuals can easily skirt financial disclosure or tax requirements, creating new opportunities for tax evasion and off-shoring. They are also particularly difficult to regulate and police – payment systems may be built on complex infrastructure that spans multiple jurisdictions, creating a lack of clarity on responsibility for financial compliance and supervision.[37] Many virtual currencies, especially those based on distributed ledger technologies, have no central intermediary – and therefore no 'focal point' for regulatory efforts.[38] These features have already made cryptocurrencies the currency of choice in some forms of cyber-related criminal activity, from the purchase of drugs on Silk Road to the payment of ransoms in cyberattacks.[39]

As virtual currencies become a larger part of the global economy, they will not only provide new opportunities for illicit financial flows – they may also impact the ability of states to govern currency markets and collect tax revenue. In the near-term, this raises significant concerns about financial integrity, regulatory policy, consumer protection and tax evasion. In the longer term, this may also have significant implications for macroeconomic policy, and, eventually, may impact financial stability, especially in developing countries.[40]

Corruption, criminality and development

All of these new challenges may open up new opportunities for criminal governance. But the state itself may also play a critical role in creating these opportunities.[41] A recent brief on the role of organized crime in public service delivery observed that 'it tends to be the state – through its absence or complicity – that opens the space for organized crime to gain legitimacy through service provision'.[42] In some cases, the state may simply lack the capacity to ensure environmental and resource security, deliver services to urban centres, or provide assistance to the unemployed. Yet in other cases, this failure is the result of corruption and poor governance, not under-capacity or under-resourcing.

Systemic corruption creates new entry points for criminal actors in governance and undermines development efforts. High levels of corruption weaken the effectiveness of state institutions by diverting resources to state elites or criminal actors, rather than to the provision of social services and protection. There is increasing evidence, for example, that systemic corruption has severely undermined military effectiveness in countries such as Nigeria, Mali, Afghanistan, and Ukraine.[43] It also perpetuates and exacerbates inequality: hampering economic development, diminishing state revenues through graft and tax evasion, and diverting money from social services, education, and other programs targeted at the poor. And it undermines the legitimacy of the state: as state institutions are bent crooked to funnel criminal rents into the pockets of national elites – rather than to provide services and protection to the population – citizens lose their faith in the willingness or desire of the government to act in their best interests. Efforts to address future vulnerabilities in developing states may, then, be significantly undermined by high levels of corruption.

1.2 Policy implications

Crooked States suggests that policy choices that ensure that states, working with civil society and legitimate business, provide protection and reduce vulnerabilities will be key to preventing and reducing the governmental influence of criminal actors. This points to several policy implications.

Use social protection policies to address vulnerabilities

First, reducing the impact of organized crime and corruption requires solutions that go beyond narrowly technical programming aimed at law enforcement or the security sector. Criminal groups gain legitimacy 'by meeting fundamental needs for livelihoods, security, and justice more successfully and consistently than the state'.[46] Policies and programming that address vulnerabilities, provide broad social protections and promote good governance – in areas from climate change to labour markets – are key to ensuring that protection needs are served by legitimate actors, rather than by criminal interests. This may include economic livelihood programming, social protection policies and other economic interventions designed to ensure the equitable distribution of resources (including taxation policy), or investment in social-service provision and infrastructure development in new urban areas. This may also require a re-evaluation of thinking around the role of the state in service provision. For much of the past three decades, the policies that emerged from the Washington Consensus have encouraged the privatization of social service provision and reductions in government spending – leaving many communities vulnerable and under-served by the state. This has, in turn, created space for criminal actors to provide public services and gain social legitimacy in these communities.[48]

Minimize the criminalizing impact of labour market disruptions

Secondly, it will require that policy interventions are designed to counter tomorrow's vulnerabilities, not just today's. Development actors increasingly consider economic livelihoods and targeted socio-economic programming as critical to reducing the scale and impact of organized crime.[49] But such programming should take into consideration the potential disruptive impacts of automation and artificial intelligence on labour markets. Livelihood or job-training programming should focus on building skills and training workers for the jobs of tomorrow, including care-intensive jobs, or jobs that require higher levels of creativity and agile thinking.[50] International organizations, such as multilateral development banks, may also begin to consider alternative forms of livelihood provision, such as the possibility of universal basic income.

Use anti-corruption interventions

Systemic corruption undermines the social contract between citizens and the state, and weakens state legitimacy – opening up opportunities for other providers of governance. There is a clear need for interventions aimed at reducing corruption and poor governance.[51] Addressing corruption requires a multi-faceted approach: on the most basic level, for example, aid targeted at promoting environmental and economic resilience should include provisions for ensuring transparency and proper management of funds. But international actors should also focus on addressing impunity and promoting good governance, including through more strategic interventions addressing the links between corruption and political finance, and working out when strategic communication can be used to delegitimize corrupt behaviour and shift social norms to promote resilience to organized crime.[52] And some existing preferences in development policy – for example in favour of decentralization – may need re-examination. There is growing evidence that decentralization in developing and post-conflict states can facilitate the organization of crime, unless matched by adequate anti-corruption resources.[53]

Strengthen the role of global finance in development outcomes

Finally, addressing corruption and reducing opportunities for criminality in governance will also require coordinated action to stem illicit financial flows. Financial deregulation has helped to facilitate the easy and opaque movement of large amounts of capital – and, in turn, made it easier for state elites to hide illicit proceeds, or to use global markets to mask grand corruption or facilitate collusion with criminal elements.[54] The majority of illicit financial outflows from developing countries end up in banks in developed countries such as the United Kingdom or the United States, or in offshore financial centres.[55] Addressing grand corruption, therefore, will also require more decisive efforts by wealthy countries to improve financial transparency and minimize the use of offshore tax havens.[56]

Efforts to improve regulation and minimize illicit financial flows have increased in recent years. Policies have been enacted to require automatic disclosure of tax information, improve transparency measures in the banking sector, and implement new standards for effective anti-money laundering practices.[57] But while these efforts have found some success, there are also significant limitations. Combatting illicit financial flows requires coordination across sectors and national borders.[58] Anti-money laundering regulations, for example, are only as strong as their weakest link – creating loopholes in countries where compliance or enforcement is weak.[59] And attempts to crack down on illicit financial flows through cooperation with financial institutions have led to an increase in other, less regulated forms of illicit value transfers, such as using high-value commodities (including art, luxury vehicles or real estate) to launder money.[60] Policymakers should also begin to consider the regulatory and governance challenges posed by this rise in virtual currencies.[61]

2. Stabilization and peacebuilding

Conventional wisdom once held that criminal and political actors were entirely distinct – that criminal groups had purely economic, not political, motivations, and therefore played a limited role in conflict. But there is increasing recognition that this distinction is not always entirely accurate: some criminal groups may not only meddle in politics for instrumental reasons, but also develop political goals and motivations; while political actors sometimes draw their political and economic power, in part, from illicit economic activity.[62] The distinction is especially blurred in times of conflict and post-conflict transitions. War is, fundamentally, a competition for legitimacy, and for governmental power. Societies that are in, or emerging from, conflict, are societies where the state has 'retreated', or otherwise failed to monopolize the provision of protection and governance – and where multiple actors, with multiple motivations – many of them using criminal means and methods – compete to fill this governmental role.[63] The ways in which post-conflict transitions are managed – and the political settlements that result – may determine whether organized criminality becomes an entrenched component of the political order in those contexts for decades to come.[64]

2.1 How conflict and transitions facilitate organized crime and corruption

This requires understanding the ways in which conflict creates opportunities and entry points for organized crime and corruption – and, in turn, how organized crime may influence conflict dynamics or hinder peace processes and post conflict recovery.

War is criminogenic

War confers legitimacy on predation and criminal activity. Conflict weakens norms around the use of violence and coercion, and weakens the allegiance of individuals to the state.[65] The proliferation of weapons and individuals trained

in violence also provides ready fodder for criminal groups, lowering 'the costs of developing alternative, non-state sources of protection'.[66] And in the post-conflict period, high levels of predatory criminality, such as rape, robbery or extortion may further fuel criminal dynamics and undermine the legitimacy of newly formed or nascent governments.[67] Vanda Felbab-Brown, for example, argues that the transitional government's failure to combat – and in some cases, tacit endorsement of – predatory criminality in Afghanistan undermined stabilization efforts. This failure created space for the resurgence of the Taliban, which gained social legitimacy by presenting itself as 'a more predictable and less corrupt ruler'.[68]

Crime as survival and coping strategy

Conflict also breaks down the distinction between licit and illicit economies. Shortages of food and other goods may lead to the proliferation of black markets, while lack of economic opportunity may erode normative barriers against participation in criminal activity.[69] Criminal groups may offer protection against economic insecurity, not only facilitating the provision of food, water, or other critical resources, but also offering one of the only available means of economic opportunity.[70]

The criminal rents to be extracted from illicit flows are particularly valuable during conflict. Both state and non-state actors may seek to ally themselves with, or co-opt, the groups that control access to these rents. This, in turn, can often lead to new forms of partnership and collaboration between organized criminal groups and the state. The allegiances of individual actors may shift between the state, non-state armed groups, and criminal groups, while criminal and political motivations may be difficult to distinguish.[71]

Criminal subversion of transitions

Collaboration often extends beyond purely financial considerations. The local legitimacy that organized criminal groups gain during conflict – from their control over illicit economies, the provision of livelihoods, and, often, the protection and services that they may offer to local communities – is particularly appealing to political actors seeking to secure power in the post-conflict political order.[72] These actors may choose to partner with criminal networks to reach and govern local populations – for example, during electoral processes in the post-conflict period. Criminal groups may use their governmental reach and coercive power to garner votes and economic support for politicians in exchange for influence or favourable treatment down the line, and may even wield this influence during the negotiation of political settlements.[73]

2.2 Policy implications

Some key policy implications emerge.

Crime-proof stabilization efforts

First, stabilization and peacebuilding actors must recognize that their interventions have complex local impacts on political economies – including the illicit aspects of those political economies. Without a stronger understanding of how interventions impact local criminal markets, those interventions risk reinforcing or conferring legitimacy on criminal behaviour, or directly or indirectly contributing to criminal networks. It is now well recognized that some stabilization policies adopted in Afghanistan over the last decade, for example, may have contributed to the criminalization of governance.[74] Contemporary interventions in Libya may carry similar risks.[75]

International actors must ensure that their interventions 'do no crime': that interventions by third-party actors do not inadvertently promote opportunities for organized crime.[76] A detailed understanding of the local political economy, for example, can help guard against the possibility that peace operations, procurement, and aid provision bolster illicit flows.[77] Early work on this issue in multilateral peace operations could and should be expanded to the broader development context.

Strategic engagement of groups with criminal agendas

A more effective approach to managing criminal agendas in stabilization will also require weighing the positives and negatives of engaging with such actors. Interventions should consider when and how to involve actors with criminal agendas in peace negotiations, just as they often consider whether to engage with rebel groups during peace processes. (Indeed, these are often the same groups.)[78] In some cases, engaging these actors risks legitimizing criminal behaviour and inadvertently benefiting criminal networks. But criminal groups may also wield significant political power, and omitting them from negotiations may risk creating criminal spoilers in the peace process.[79]

Engaging with criminal actors may, in many cases, be politically controversial. But criminal actors can still be rational actors, and may be responsive to incentives and inducements aimed to motivate them to abandon undesirable behaviour.[80] This may include creating opportunities for such actors in the licit economy during periods of post-conflict recovery. A recent analysis of protection economies in Somalia, for example, found that when the available profits from protecting licit trade outweighed the profits from protecting piracy, local elites turned away from supporting criminality.[81] Significant further research and controlled innovation in this field is required to understand what works.

Build effective governance – not just government

Finally, peacebuilding and stabilization programming may require a greater focus on promoting 'governance', rather than 'government'. Often, interventions are aimed at shoring up the legitimacy of the state, promoting state-based governance or 'extending state authority'.[82] But in the aftermath of conflict, the 'state' often remains a contested concept. Non-state actors, including political or criminal

groups, may compete with state actors for the allegiance of citizens.[83] Criminals may supply critical social services and protection[84] - as well as much-needed meaning and identity to citizens in the aftermath of conflict.[85] In some cases, international actors may attempt to harness the social and political power of these groups, leaving governance structures in place while offering incentives to renounce criminal behaviour.[86]

3. Cyber-development and cyber-inequality

Cyberspace and digitization are increasingly central to every aspect of social and political life. In the next five years, more than one billion new internet users may come online, driven primarily by growth in low- and middle-income countries.[87] And as more and more everyday items are connected to the internet, digitization will affect virtually every industry. In 2015, approximately 20 billion devices were connected to the Internet; by 2020, this number may rise to 40 billion. These technological changes are leading to a reorganization of geo-economic power and disrupting global value chains in ways that have significant implications for the future of organized crime and corruption in developing states.

Development efforts have only recently begun to take into account the impact of this increasingly ubiquitous digitization, and how technology is changing our understanding of security, social inclusion, and state-citizen relationships. Understanding the intersection of criminality, cyberspace and development includes understanding how choices around 'cyberdevelopment' may enable illicit activity and facilitate new forms of criminality. But it also requires consideration of where new vulnerabilities will arise, and what new demands for protection may emerge as a result.

3.1 How changes in cyberspace may facilitate organized crime and corruption

The implications of cyberspace for development are beginning to emerge.

Developing countries are testing grounds for cybercrime

First, it is increasingly clear that the question of cyber-vulnerability and the threat of cybercrime is not confined to specific industries and regions. The May 2017 'WannaCry' ransomware attack, for example, affected more than 150 countries[90] – highlighting the vulnerability of a range of industries in low- and high-income countries alike, and demonstrating the potential destabilizing effects of such attacks. Keeping pace with rapidly changing cyber-threats requires significant resources, and developing states may struggle to update critical technical infrastructure or upgrade cybersecurity capabilities, leaving them especially vulnerable to attack. Networks are generally most vulnerable when new technologies are grafted onto legacy systems, for example, posing particular threats for industries with large, outdated technological systems, such as the healthcare, educational, and agricultural sectors.[91] For this very reason, developing countries may be treated by cybercriminals as testing grounds.[92]

Cyber-enabled crimes, or traditional crimes that have become cyber, will also pose a growing challenge for developing countries, especially for law enforcement and security sectors. Many traditional organized crime groups increasingly use the Internet to facilitate some form of their illicit activity: recruiting new members, buying fake identities, selling illicit goods, or laundering ill-gotten gains.[93] And, as discussed above, the rise in digital finance has already made it easier for criminal groups and corrupt actors to quickly and easily obscure the provenance of criminal rents, and to more readily evade regulators and law enforcement.[94] As cyber-connectivity in developing countries becomes more robust, larger swaths of illicit trafficking networks, such as those for drugs, arms or people, will likely move online. Criminal actors may 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.[95] Law enforcement institutions in developing countries, which often have more rudimentary technological capabilities, may struggle to police criminality in cyberspace. This also poses challenges for developing countries' electoral institutions, which, as the recent elections in Kenya show, may be vulnerable to hacking

Cybercrime and cyber-inequality

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 start-up costs – often just the price of a computer and an internet connection, with user-friendly malware increasingly widely available.[96] Low-level cyber-criminality may become increasingly widespread – especially in countries where economic opportunities in the licit economy are limited – as the next billion people come online. Cybercrimes such as fraud and intellectual property theft, for example, already provide livelihoods to significant numbers of people in countries such as Ghana, Nigeria, and Cameroon.[97]

But the way in which new forms of criminality and criminal organization develop will depend on how cyberspace itself evolves. Distributed ledger technology may actually reduce opportunities for large-scale internet fraud or theft, such as last year's multimillion dollar theft from the Bank of Bangladesh.[98] Instead, there may be a rise in low-value, predatory cybercrime that targets end users, increasing individual insecurity in cyberspace.

In a world that is permanently online, digital footprints and signatures are highly valuable commodities, and an array of public and private actors will be interested in accessing or

controlling this data. Governments, for example, increasingly use communication data to monitor the activities of their citizens.[99] Private companies, from health care companies to internet service providers, also routinely buy and sell consumer data to target advertising or guide investments.[100] And for criminal actors, personally identifiable information offers numerous opportunities for the extraction of criminal rents – from identity fraud to ransomware attacks.

The growing ubiquity of digital data will create new demands for protection. The lines between the licit and illicit marketplaces for personal data, for example, may be increasingly blurred, as both criminal groups and legal 'data brokers' buy and sell personal data in online exchanges.[101] In many cases, governments do not offer much insurance against this protection: the laws that govern different types of data collection are often vague or outdated, and vary significantly from country to country.[102] Instead, much of this cyber-protection is provided not by state actors, but by private, commercial actors, such as cybersecurity companies. Those who cannot pay will be subject to high levels of insecurity and vulnerability.

This also leads us to consider what poverty, social exclusion and inequality may look like in an increasingly digital world. Cyberspace and digital access are increasingly critical to innovation and economic development, and digital connectivity offers an array of social, economic and civic benefits to individuals.[103] Significant portions of the developing world, however, still remain excluded from this space, as high costs, poor infrastructure and other barriers impede universal internet access.[104] As access expands, there are questions about what form it may take. Increasingly, for example, initiatives from private companies such as Google and Facebook offer free but highly restricted internet connectivity in the developing world. Access is limited to only pre-approved portions of the internet – often to their own proprietary sites – while expanded access requires additional fees.[105] Such unequal access models, if widely adopted, risk 'entrenching and amplifying existing inequalities' and contributing to the social exclusion of low-income or marginalized populations from the global community.[106]

Increasingly, the very machinery of commerce may depend on a cybermachinery owned and operated by organizations in the global North. Developing country actors' access may be predicated upon their willingness to surrender data sovereignty. This risks leading to cyberspace not serving as a platform for innovation and development, but for entrenchment of inequality and exclusion.

Cyberspace as a platform for new forms of international governance

Today, the Internet is often thought of as a 'global commons', while it increasingly functions more like a 'club' dominated by a limited number of actors. States are increasingly controlling what parts of the Internet, and what content, their citizens can access, using cyber-protection to justify interposing themselves between people and the Internet.[107] Other states are actively supporting the maintenance of open spaces and services and agreeing to global standards and regulations around internet access, data security, and cyber-conflict.[108] Either way, developing states may struggle to protect their cyber-borders, just as today they often struggle to protect their physical ones. Citizens in weak states may therefore face more insecurity and be more vulnerable to cyber-criminality – or they may be more willing to pay other actors for protection. And as value chains become increasingly digital, developing states may struggle to protect or police these value chains. The rise of virtual currencies and peer-to-peer payment systems may further compound these challenges, posing acute challenges for state control of economic value and financial security.

New forms of cooperation may emerge between state, local and private actors in response to this insecurity. Some states or municipalities, for example, could choose to partner with commercial actors to create highly protected economic and cyber spaces, within which protection and trust services are provided to a geographically dispersed but closed-off network.[109] This would likely challenge the economic and political power of some developing countries. It could, for instance, create zones of exclusion, in which some communities are left out of these protected networks, instead existing in a heightened state of economic and cyber-insecurity. It could also lead to new forms of dependency, as developing states are forced to rely on richer states or transnational corporations for secure access to cyberspace and cyber-capabilities.

3.2 Policy implications

A few key implications arise.

Bolster cyber defences in developing states

Cybersecurity will be increasingly central to promoting resilience and security in developing countries. The anonymous and cross-border nature of cyberspace has made it challenging for state institutions, even in wealthy states, to keep up with and provide protection against new forms of vulnerability. In developing states where capacity is limited, this may prove even more difficult. There will likely be a need for development assistance that helps low-income countries bolster their cyber defences, provides education on cyber-hygiene and other best practices, and improves the cyber capacity of security institutions.[110] Because so much of the infrastructure of the internet is owned and operated by private companies, public-private cooperation will also be key to investing in and implementing updated cybersecurity measures.[111] International actors may be well-positioned to help facilitate cooperation with transnational corporations and service providers, and to ensure that cybersecurity standards enforced in their own countries are applied across the network.

Leverage technology to improve development outcomes

Development efforts should also begin to focus on helping developing states harness the positive impacts of technology and cyberspace to promote good governance and foster economic and social resilience. This may include re-training or re-educating workers in new and emerging technologies, and fostering the development of new industries. such as robotics and additive manufacturing. In China, for example, where manufacturing jobs are at high risk of automation, the government has taken an active role in developing the domestic robot industry.[112] Additive manufacturing, similarly, may significantly disrupt current patterns of global manufacturing and production – but with lower start-up costs and overhead than traditional manufacturing, it may also offer new opportunities for development and innovation in low-income countries.[113] Blockchain technologies may also lower barriers to entry for entrepreneurs. Developing country entrepreneurs will only be able to compete, however, if they are exposed to these new technologies sufficiently early, and given access to the reliable broadband service that is needed to harness those technologies.

Development assistance could also promote the use of technology to increase transparency and improve government effectiveness, while also reinforcing cybersecurity. Some governments, for example, are experimenting with using blockchain – the distributed ledger technology that underpins Bitcoin – to secure government records and protect citizen privacy.[114] One such initiative in Georgia uses blockchain to create a transparent and reliable land registry system, designed to guarantee the property rights of citizens.[115] Other technologies may help to improve service delivery while providing protections for personal data and individual privacy. In Estonia, for instance, government-issued, secure electronic ID cards allow citizens to safely access healthcare, conduct business over the internet, and file their taxes.[116] The ID2020 Initiative, similarly, is using biometric data and blockchain technology to build a digital platform that will provide legal, digital identities for vulnerable populations, including refugees and victims of modern slavery.[117] While these initiatives are relatively nascent, such programming may help to reduce vulnerabilities and bolster the ability of the international community to cooperate to provide protection against insecurity.

Consider global cyber-governance

The conclusions reached in *Crooked States* and throughout this brief also indicate a need to think more expansively about the future of cyber-governance, and to consider how multi-stakeholder arrangements may help to promote security and provide protection against vulnerabilities, including those arising from cybercrime.

Today, cyber-governance is at a crossroads: both states and private actors are just beginning to consider what norms and legal protections should govern behaviour in cyberspace.[118] And high-income states are increasingly making policy choices about Internet access and data protection within their own borders. But this *ad hoc* approach risks entrenching the potentially harmful dynamics discussed above, and leading to new forms of inequality and vulnerability in developing states.

Instead, state and private institutions should cooperate to collectively protect cyberspace as a *global* commons. This would require strengthened governance to ensure equal access and promote a rules-based, safe and accessible internet, minimizing the role played by cybercrime, and protecting the open nature of the Internet as a global public good.[119] Critically, this will require involving private businesses and corporations that produce, distribute, own and operate key parts of the infrastructure of cyberspace. Any attempts to implement cyber-governance agreements will require cooperation and buy-in from these actors. States will need to find ways to establish and maintain incentive structures and accountability systems that motivate private actors to help protect cyberspace as an open space for innovation and individual activity.

Development actors should also help ensure that future cyber-governance reflects the interests of developing states, and that it helps to address new forms of cybercrime vulnerability in small and low-income states. This may require promoting principles of net neutrality and global data protection laws. It will also require discouraging policies that lead to increased fragmentation in cyberspace – such as data localization laws that may inhibit the free flow of data[120] and create rent-extraction opportunities for local criminal actors – while advocating for more robust, but flexible, data protections. Finally, it may involve active measures to ensure the effective representation of smaller developing states in such multi-stakeholder initiatives. Technical and financial support, for example, could be provided to both private and public actors from developing states who would otherwise struggle to meaningfully participate in governance arrangements.[121]

ENDNOTES

[1] Sarah Chayes, *Thieves of State: Why Corruption Threatens Global Security* (New York: W.W. Norton & Company, Inc., 2015).
[2] Tuesday Reitano and Marcena Hunter, "Protecting Politics: Deterring the Influence of Organized Crime on Public Service Delivery" (Stockholm / Geneva: Global Initiative Against Transnational Organized Crime and International IDEA, 2016).
[3] Mark Shaw, Tuesday Reitano, and Marcena Hunter, "Development Responses to Organized Crime: An Analysis and Programme Framework."11.
[4] Letizia Paoli, *The Oxford Handbook of Organized Crime* (Oxford University Press, 2014).
[5] For a larger discussion of this definition and its limitations, please see *Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now*. For additional information on criminal rents, see also Thomas Schelling, 'What is the Business of Organized Crime?', *J. Pub. Law*, vol. 20, no. 1 (1970), pp. 71-84; Jean Cartier-Bresson, 'État, Marchés, Réseaux et Organisations Criminelles Entrepreneuriales', Paper presented at the Colloquium on 'Criminalité Organisée et Ordre dans la Societé', Aix-en-Provence, 5-7 June 1996 (Aix-en-Provence: Aix-Marseille University Press, 1997); Gianluca Fiorentini and Sam Peltzman, 'Introduction', in Fiorentini and Peltzman, eds., *The Economics of Organized Crime* (Cambridge: Cambridge University Press, 1995/1997), pp. 1-30; and R.T. Naylor, *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy* (Ithaca and London: Cornell University Press, 2004, revd ed.), p. 15.
[6] See Frank G. Madsen, 'Corruption: A Global Common Evil', The RUSI Journal, vol. 158, no. 2 (2013), pp. 26-38.
[7] Federico Varese, "General Introduction: What Is Organized Crime?," in *Organized Crime: Critical Concepts in Criminology*, ed. Federico Varese (London: Routledge, 2010); Mark Shaw, "'We Pay, You Pay': Protection Economies, Financial Flows, and Violence," in *Beyond Convergence: World Without Order*, ed. Hilary Matfess and Michael Miklaucic (Washington D.C.: National Defense University Press, 2016), 235–50.
[8] Mark Shaw, Tuesday Reitano, and Marcena Hunter, "Development Responses to Organized Crime: An Analysis and Programme Framework" (Global Initiative Against Transnational Organized Crime, April 2016). 11.
[9] James Cockayne, *Hidden Power: The Strategic Logic of Organized Crime* (New York: Oxford University Press, 2016).
[10] Judith Vorrath, "Organized Crime and Development: Challenges and Policy Options for West Africa's Fragile States," SWP Research Paper, trans. Hillary Crowe (Berlin, Germany: Stiftung Wissenschaft und Politik - German Institute for International and Security Affairs, December 2015).
[11] Lauren Van Metre, "Fragility and Resilience," Policy Brief (Fragility Study Group, September 2016), https://www.usip.org/sites/default/files/Fragility-Report-Policy-Brief-Fragility-and-Resilience_0.pdf; Mark Shaw, "'We Pay, You Pay': Protection Economies, Financial Flows, and Violence."
[12] "Trends Transforming the Global Landscape," *Director of National Intelligence*, accessed April 11, 2017, https://www.dni.gov/index.php/global-trends/trends-transforming-the-global-landscape.
[13] For an in-depth summary of the trends impacting global food supply, see Food and Agriculture Organization of the United Nations, "The Future of Food and Agriculture: Trends and Challenges" (Food and Agriculture Organization of the United Nations, 2017), http://www.fao.org/3/a-i6881e.pdf. and FAO Regional Conference for Europe, "Global Trends and Future Challenges for the Work of the Organization," 2012.
[14] UK Ministry of Defence, "Global Strategic Trends - Out to 2045," DCDC Strategic Trends Programme (Ministry of Defence, June 30, 2014), https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045. 22.
[15] Boekhout van Solinge, 'The Illegal Exploitation of Natural Resources'. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199730445.001.0001/oxfordhb-9780199730445-e-024
[16] Aman Sethi, "At the Mercy of the Water Mafia," *Foreign Policy*, accessed May 5, 2017, https://foreignpolicy.com/2015/07/17/at-the-mercy-of-the-water-mafia-india-delhi-tanker-gang-scarcity/; Nicole Johnston, "Karachi 'Water Mafia' Sucking City's Pipelines Dry - Al Jazeera English," *Al Jazeera*, September 10, 2015, http://www.aljazeera.com/news/2015/09/karachi-water-mafia-sucking-city-pipelines-dry-150910062202773.html.
[17] David Kilcullen, "The City as a System: Future Conflict and Urban Resilience," *The Fletcher Forum of World Affairs* 36, no. 2 (Summer 2012): 19–39.
[18] Robert Muggah, "Where Are the World's Most Fragile Cities?," *Igarapé Institute*, September 12, 2016, https://igarape.org.br/en/where-are-the-worlds-most-fragile-cities/.
[19] John de Boer, Robert Muggah, and Ronak Patel, "Conceptualizing City Fragility and Resilience," Working Paper (United Nations University Centre for Policy Research, October 2016).
[20] Mediel Hove, Emmaculate Ngwerume, and Cyprian Muchemwa, "The Urban Crisis in Sub-Saharan Africa: A Threat to Human Security and Sustainable Development," *Stability: International Journal of Security and Development* 2, no. 1 (March 11, 2013), doi:10.5334/sta.ap.
[21] Mark Shaw and Simon Howell, "Governing Safer Cities: Strategies for a Globalised World" (United Nations Office on Drugs and Crime, December 2016), http://globalinitiative.net/wp-content/uploads/2017/02/unodc-safercities-feb-17.pdf.
[22] Camino Kavanagh et al., "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries" (NYU Center on International Cooperation, June 2013), http://cic.nyu.edu/sites/default/files/kavanagh_crime_developing_countries_report.pdf.
[23] Vanda Felbab-Brown, "The Purpose of Law Enforcement Is to Make Good Criminals? How to Effectively Respond to the Crime-Terrorism Nexus," *Brookings*, November 30, 2001, https://www.brookings.edu/on-the-record/the-purpose-of-law-enforcement-is-to-make-good-criminals-how-to-effectively-respond-to-the-crime-terrorism-nexus/; Mark Shaw and Simon Howell, "Governing Safer Cities: Strategies for a Globalised World."
[24] "In the Developing World, Two-Thirds of Jobs Could Be Lost to Robots," *World Economic Forum*, accessed May 10, 2017, https://www.weforum.org/agenda/2016/11/in-the-developing-world-two-thirds-of-jobs-could-be-lost-to-robots/.
[25] "Technology at Work v2.0: The Future Is Not What It Used to Be," Citi GPS: Global Perspectives & Solutions (Oxford Martin School and Citi, January 2016), http://www.oxfordmartin.ox.ac.uk/downloads/reports/Citi_GPS_Technology_Work_2.pdf.
[26] "World Population Prospects: The 2015 Revision, Key Findings and

Advance Tables," Working Paper (United Nations Department of Economic and Social Affairs, Population Division, 2015).

[27] Kai-Fu Lee, "The Real Threat of Artificial Intelligence," *The New York Times*, June 24, 2017, sec. Opinion, https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.

[28] Tuesday Reitano and Marcena Hunter, "Protecting Politics: Deterring the Influence of Organized Crime on Public Service Delivery."

[29] Colin P. Clarke, Phil Williams, and Steven Davenport, "The Future of Transnational Organized Crime" (On file with the authors, 2017).

[30] Petr Jansky, "Illicit Financial Flows and the 2013 Commitment to Development Index," CGD Policy Paper (Center for Global Development, December 16, 2013), https://www.cgdev.org/publication/illicit-financial-flows-and-2013-commitment-development-index. 7.

[31] Quentin Reed and Alessandra Fontana, "Corruption and Illicit Financial Flows: The Limits and Possibilities of Current Approaches," U4 Issue (Chr. Michelsen Institute, January 2011).

[32] Ibid.; Nils Gilman, "The Twin Insurgencies: Plutocrats and Criminals Challenge the Westphalian State," in *Beyond Convergence: World Without Order*, ed. Hillary Matfess and Michael Miklaucic (Washington D.C.: Institute for National Strategic Studies, Center for Complex Operations, 2016), 47–60; James Cockayne, "Is Unbridled Globalization Creating Mafia States?," *International Peace Institute*, October 11, 2016, https://theglobalobservatory.org/2016/10/globalization-mafia-states-organized-crime/.

[33] Dev Kar, "Financial Flows and Tax Havens" (Global Financial Integrity, December 2015), http://www.gfintegrity.org/wp-content/uploads/2016/12/Financial_Flows-final.pdf.52.

[34] Tatiana Tropina, "Do Digital Technologies Facilitate Illicit Financial Flows?," Background Paper, World Development Report 2016 Digital Dividends (Max Planck Institute for Foreign and International Criminal Law, 2016).

[35] Tim Fernholz, "How Digital Currencies Democratize Tax Evasion," *Quartz*, accessed May 11, 2017, https://qz.com/92842/how-digital-currencies-democratize-tax-evasion/, "Taming Tax Fraud's New Digital Frontier: What Can Tax Authorities Do to Take On Fraudsters and Win" (Capgemini Consulting, n.d.), https://www.capgemini-consulting.com/resource-file-access/resource/pdf/tax-fraud-paper.pdf.

[36] Dong He et al., "Virtual Currencies and Beyond: Initial Considerations," IMF Staff Discussion Note (International Monetary Fund, January 2016).

[37] Ibid; FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," Financial Action Task Force Report, (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[38] Dong He et al., "Virtual Currencies and Beyond: Initial Considerations."

[39] Ibid.

[40] Ibid.

[41] Tuesday Reitano and Marcena Hunter, "Protecting Politics: Deterring the Influence of Organized Crime on Public Service Delivery," 12.

[42] Ibid.

[43] See, for example, Eva Anderson and Matthew T. Page, "Weaponising Transparency: Defence Procurement Reform as a Counterterrorism Strategy in Nigeria" (Transparency International, May 2017), https://ti-defence.org/publications/weaponising-transparency/; Cockayne, *Hidden Power*; Chayes, *Thieves of State*; Sarah Chayes, "Corruption and State Fragility," Policy Brief (Fragility Study Group, September 2016).

[44] Sanjeev Gupta, Hamid Davoodi, and Rosa Alonso-Terme, "Does Corruption Affect Income Inequality and Poverty?," IMF Working Paper, (May 1998).

[45] Chayes, "Corruption and State Fragility."

[46] Mark Shaw, Tuesday Reitano, and Marcena Hunter, "Development Responses to Organized Crime: An Analysis and Programme Framework," 31.

[47] Louise I. Shelley, *Dirty Entanglements: Corruption, Crime, and Terrorism* (Cambridge University Press, 2014); Nils Gilman, "The Twin Insurgencies: Plutocrats and Criminals Challenge the Westphalian State"; James Cockayne, "Is Unbridled Globalization Creating Mafia States?"

[48] James Cockayne, "Is Unbridled Globalization Creating Mafia States?"

[49] Mark Shaw, Tuesday Reitano, and Marcena Hunter, "Development Responses to Organized Crime: An Analysis and Programme Framework."

[50] Alec Ross, *The Industries of the Future*, First Simon & Schuster hardcover edition (New York London Toronto Sydney New Delhi: Simon & Schuster, 2016).

[51] "Corruption: The Unrecognized Threat to International Security," Working Group on Corruption and Security (Carnegie Endowment for International Peace, 2014), http://carnegieendowment.org/files/corruption_and_security.pdf.

[52] Ivan Briscoe, Catalina Perdomo, and Catalina Uribe Burcher, eds., *Redes ilícitas y política en América Latina* (Estocolmo: Instituto Internacional para la Democracia y la Asistencia Electoral, IDEA Internacional : Netherlands Institute for Multiparty Democracy, NIMD : Netherlands Institute of International Relations, 2014); Elin Falguera et al., eds., *Funding of Political Parties and Election Campaigns: A Handbook on Political Finance* (Stockholm: IDEA, 2014).

[53] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice," Occasional Paper (United Nations University Centre for Policy Research, August 2016).

[54] Dev Kar and Devon Cartwright-Smith, "Illicit Financial Flows from Africa: Hidden Resource for Development" (Global Financial Integrity, March 2010), http://www.gfintegrity.org/storage/gfip/documents/reports/gfi_africareport_web.pdf; Nils Gilman, "The Twin Insurgencies: Plutocrats and Criminals Challenge the Westphalian State"; Nikos Passas, "Global Anomie, Dysnomie, and Economic Crime: Hidden Consequences of Globalization and Neo-Liberalism in Russia and around the World," *Social Justice* 27, no. 2 (2000): 16–44; Cockayne, *Hidden Power*; Quentin Reed and Alessandra Fontana, "Corruption and Illicit Financial Flows: The Limits and Possibilities of Current Approaches."

[55] "Illicit Financial Flows," *Global Financial Integrity*, accessed May 12, 2017, http://www.gfintegrity.org/issue/illicit-financial-flows/.

[56] Quentin Reed and Alessandra Fontana, "Corruption and Illicit Financial Flows: The Limits and Possibilities of Current Approaches."

[57] Ibid.

[58] "Coherent Policies for Combatting Illicit Financial Flows," Issue Brief Series (United Nations Office on Drugs and Crime / Organisation for Economic Co-operation and Development, July 2016), http://www.un.org/esa/ffd/wp-content/uploads/2016/01/Coherent-policies-for-combatting-Illicit-Financial-Flows_UNODC-OECD_IATF-Issue-Brief.pdf.

[57] Quentin Reed and Alessandra Fontana, "Corruption and Illicit Financial Flows: The Limits and Possibilities of Current Approaches."

[60] Max Heywood, "Tainted Treasures: Money Laundering Risks in Luxury Markets" (Transparency International, March 2017), https://www.transparency.org/whatwedo/publication/tainted_treasures_money_laundering_risks_in_luxury_markets.
[61] Quentin Reed and Alessandra Fontana, "Corruption and Illicit Financial Flows: The Limits and Possibilities of Current Approaches."
[62] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice."
[63] We are indebted to Prof Mats Berdal for the conversation that helped shape the arguments in this section.
[64] Camino Kavanagh et al., "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries"; James Cockayne, "Can Organized Crime Shape Post-War Transitions? Evidence from Sicily," ed. Sabine Kurtenbach and Angelika Rettberg, *Third World Thematics*, Forthcoming; Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice."
[65] Cockayne, *Hidden Power*; Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice."
[66] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice," 3.
[67] Ibid.; Camino Kavanagh et al., "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries."
[68] Vanda Felbab-Brown, "Afghanistan Affectations: How to Break Political-Criminal Alliances in Contexts of Transition," Crime-Conflict Nexus Series (United Nations University Centre for Policy Research, April 2017), https://i.unu.edu/media/cpr.unu.edu/attachment/2442/Afghanistan-Affectations-How-to-Break-Political-Criminal-Alliances-in-Contexts-of-Transition.pdf.
[69] Cockayne, *Hidden Power*; Cockayne, "Can Organized Crime Shape Post-War Transitions? Evidence from Sicily."
[70] Clarke, Williams, and Davenport, "The Future of Transnational Organized Crime."
[71] See, for example, recent publications in the UNU Crime-Conflict Nexus Project: Vanda Felbab-Brown, "The Hellish Road to Good Intentions: How to Break Political-Criminal Alliances in Contexts of Transition," Crime-Conflict Nexus Series (United Nations University Centre for Policy Research, April 2017); James Cockayne, John de Boer, and Louise Bosetti, "Going Straight: Criminal Spoilers, Gang Truces and Negotiated Transitions to Lawful Order," Crime-Conflict Nexus Series (United Nations University Centre for Policy Research, April 2017); John de Boer, Juan Carlos Garzón-Vergara, and Louise Bosetti, "Criminal Agendas and Peace Negotiations: The Case of Colombia," Crime-Conflict Nexus Series (United Nations University Centre for Policy Research, April 27, 2017).
[72] "The Crime-Conflict 'Nexus': State of the Evidence," Occasional Paper (United Nations University Centre for Policy Research, July 2015).
[73] Cockayne, "Can Organized Crime Shape Post-War Transitions? Evidence from Sicily."; Ivan Briscoe, "Protecting Politics: Deterring the Influence of Organized Crime on Elections," accessed June 9, 2017, http://www.idea.int/publications/catalogue/protecting-politics-deterring-influence-organized-crime-elections; Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice."
[74] Vanda Felbab-Brown, "Afghanistan Affectations: How to Break Political-Criminal Alliances in Contexts of Transition."
[75] Tuesday Reitano and Mark Shaw, "Libya: The Politics of Power, Protection, Identity and Illicit Trade," Crime-Conflict Nexus Series (United Nations University Centre for Policy Research, May 2017), https://i.unu.edu/media/cpr.unu.edu/attachment/2523/Libya-The-Politics-of-Power-Protection-Identity-and-Illicit-Trade-02.pdf.
[76] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice," 3.
[77] Ibid.
[78] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice"; James Cockayne, John de Boer, and Louise Bosetti, "Going Straight: Criminal Spoilers, Gang Truces and Negotiated Transitions to Lawful Order."
[79] James Cockayne, John de Boer, and Louise Bosetti, "Going Straight: Criminal Spoilers, Gang Truces and Negotiated Transitions to Lawful Order."
[80] Ibid.
[81] Anja Shortland and Federico Varese, "The Protector's Choice: An Application of Protection Theory to Somali Piracy," *The British Journal of Criminology* 54, no. 5 (September 1, 2014): 741–64, 760.
[82] Mark Shaw, Tuesday Reitano, and Marcena Hunter, "Development Responses to Organized Crime: An Analysis and Programme Framework."
[83] Louise Bosetti, James Cockayne, and John de Boer, "Crime-Proofing Conflict Prevention, Management, and Peacebuilding: A Review of Emerging Good Practice."
[84] Anja Shortland and Federico Varese, "State-Building, Informal Governance and Organised Crime: The Case of Somali Piracy," *Political Studies* 64, no. 4 (December 1, 2016): 811–31, 3.
[85] James Cockayne, John de Boer, and Louise Bosetti, "Going Straight: Criminal Spoilers, Gang Truces and Negotiated Transitions to Lawful Order."
[86] Ibid.
[87] John Garrity, "Internet User Growth Over the Next Five Years," *Huffington Post*, June 22, 2016, http://www.huffingtonpost.com/john-garrity/internet-user-growth-over_b_10603196.html.
[88] UK Ministry of Defence, "Global Strategic Trends - Out to 2045." 57.
[89] See, for example, the International Multilateral Partnership Against Cyber Threats (ITU-IMPACT), a public-private partnership with the United Nations' International Telecommunication Union; the International Cyber Security Prevention Alliance (ICSPA), which provides cybersecurity assistance to law enforcement agencies and governments around the world; and Close the Gap's ICT4Development program, which seeks to bridge the digital divide and advance the achievement of the Sustainable Development Goals by increasing access to information and communication technologies in the developing world.
[90] Matt Willis, "WannaCry: The Ransomware Attack on the NHS and What We Can Learn from It," *British Politics and Policy at LSE*, June 11, 2017, http://blogs.lse.ac.uk/politicsandpolicy/wannacry-the-ransomware-attack-on-the-nhs-and-what-we-can-learn-from-it/.
[91] Min-Seok Pang and Hüseyin Tanriverdi, "Security Breaches in the U.S. Federal Government," SSRN Scholarly Paper (Rochester, NY: Social

Science Research Network, March 7, 2017), https://papers.ssrn.com/abstract=2933577.

[92] Sheera Frenkel, "Hackers Find 'Ideal Testing Ground' for Attacks: Developing Countries," *The New York Times*, July 2, 2017, sec. Technology, https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html.

[93] Kim-Kwang Raymond Choo and Peter Grabosky, "Cyber Crime," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, October 15, 2013), https://papers.ssrn.com/abstract=2340803; Peter Grabosky, "Organised Crime and the Internet," *The RUSI Journal* 158, no. 5 (October 1, 2013): 18–25, doi:10.1080/03071847.2013.847707 ; Mike McGuire and Samantha Dowling, "Cyber Crime: A Review of the Evidence," Research Report (Home Office, October 2013), https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn36762-eng.pdf.

[94] Tatiana Tropina, "Do Digital Technologies Faciliate Illicit Financial Flows?"

[95] Clarke, Williams, and Davenport, "The Future of Transnational Organized Crime."

[96] David S. Wall, "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime," *The European Review of Organised Crime* 2, no. 2 (2015): 71–90.

[97] Philippa Garson, "Cybercriminals Find Wonderland in Developing Countries," *openDemocracy*, December 10, 2013, http://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries; Camino Kavanagh et al., "Getting Smart and Scaling Up: Responding to the Impact of Organized Crime on Governance in Developing Countries."

[98] Michael Corkery and Matthew Goldstein, "North Korea Said to Be Target of Inquiry Over $81 Million Cyberheist," *The New York Times*, March 22, 2017, sec. DealBook, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html.

[99] "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf; Olga Khazan, "Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says," *The Atlantic*, June 6, 2013, https://www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/.

[100] Adam Tanner, "How Data Brokers Make Money Off Your Medical Records," *Scientific American*, accessed June 9, 2017, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

[101] Adam Tanner, "How Data Brokers Make Money Off Your Medical Records," *Scientific American*, accessed June 9, 2017, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/.

[102] Khazan, "Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says."

[103] Darrell M. West, "Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content" (Brookings Institution, February 2015), https://www.brookings.edu/wp-content/uploads/2016/06/West_Internet-Access.pdf.

[104] Ibid.

[105] Lily Hay Newman, "Net Neutrality, Internet Access Is Already in Trouble in the Developing World.," *Slate*, January 21, 2014, http://www.slate.com/blogs/future_tense/2014/01/21/net_neutrality_internet_access_is_already_in_trouble_in_the_developing_world.html.

[106] Ibid.

[107] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Spring 2011, 35. Rory Cellan-Jones Lee Dave, "Iran Rolls out Domestic Internet," *BBC News*, August 29, 2016, sec. Technology, http://www.bbc.com/news/technology-37212456.

[108] See, for example, "Key Issues for Digital Transformation in the G20," Report prepared for a joint G20 German Presidency/ OECD conference (Berlin, Germany: OECD, January 12, 2017).

[109] Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I*, 2 edition (Chichester, West Sussex ; Malden, MA: Wiley-Blackwell, 2009), xviii.

[110] Lilly Pijnenburg Muller, "Cyber Security Capacity Building in Developing Countries," Policy Brief, Cybersecurity and Developing Countries (Norwegian Institute of International Affairs, 2015).

[111] Ibid.

[112] "China's Robot Revolution," *Financial Times*, accessed May 7, 2017, https://www.ft.com/content/1dbd8c60-0cc6-11e6-ad80-67655613c2d6.

[113] Avner Ben-Ner and Enno Siemsen, "Decentralization and Localization of Production: The Organizational and Economic Consequences of Additive Manufacturing (3D Printing)," *California Management Review* 59, no. 2 (February 2017): 5–23, doi:10.1177/0008125617695284; Campbell et al., "Could 3D Printing Change the World?"

[114] "Governments May Be Big Backers of the Blockchain," *The Economist*, June 1, 2017, https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers.

[115] Ibid.

[116] "Estonia Takes the Plunge," *The Economist*, June 28, 2014, https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.

[117] Jeff John Roberts, "Refugees Can Prove Who They Are With This New Technology," *Fortune*, June 19, 2017, http://fortune.com/2017/06/19/id2020-blockchain-microsoft/.

[118] Carl Bildt, "What Is the Future of Cyber Governance?," *World Economic Forum*, October 27, 2015, https://www.weforum.org/agenda/2015/10/what-is-the-future-of-cyber-governance/.

[119] See for example Sash Jayawardane, Joris Larik, and Erin Jackson, "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance," Policy Brief (The Hague Institute for Global Justice, November 2015), http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf; and Center for International Governance Innovation and The Royal Institute for International Affairs, *Global Commission on Internet Governance* (2016).

[120] The Editorial Board, "Apple and Other Tech Titans Should Tread Carefully in China," *Washington Post*, July 22, 2017, https://www.washingtonpost.com/opinions/apple-and-other-tech-titans-should-tread-carefully-in-china/2017/07/22/1734eaca-6b1e-11e7-9c15-177740635e83_story.html.

[121] Sash Jayawardane, Joris Larik, and Erin Jackson, "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance."