Careerinnovation

stars
the Stein am Rhein Symposium
for Leaders of the Next Generation

Organisations of the Future

Brief 2: What will happen to transnational crime?

Transnational crime refers to crime carried out by global networks across territorial borders. It includes money laundering, internet crime, people smuggling, the drug trade, counterfeiting and other forms of organised crime. Terrorism could be included, but is beyond the scope of this paper.

A Ci briefing paper for stars'09

Introduction

This briefing paper is one of three written specially for the next-generation international leaders taking part in **stars**'09. The papers were designed as input to a structured workshop process, to stimulate thinking on emerging issues that will impact organisations in future. The topics have been selected as examples of developments in the fields of environment/resources, politics/economics and technology.

The 2009 papers address:

1. Micro/local power generation
2. Transnational crime
3. Distributed manufacturing

Each theme is presented in the same way:

- The story so far
- What will influence the next 20 years?
- What might be the implications?

The papers are based on a review of literature and fresh interviews with selected experts, further edited to include outputs from the symposium itself. They are not designed to make precise projections, but to identify the factors that will influence developments in these fields.

Participants are welcome to use this **stars** briefing paper in their own organisations, with or without support from Ci.

About stars

The Stein am Rhein Symposium (**stars**) is a platform for "Leaders of the Next Generation" in business, science, politics and culture. **stars** creates an inspiring network and finds answers to the question "What makes a good future leader?"

www.the-stars.ch

About Ci

The Career Innovation Company (Ci) is a catalyst organisation, working with some of the world's best-known employers. Ci uses fresh research insights, collaborative events and high-impact online career and leadership tools to help them increase business agility and gain recognition as inspiring places to work.

www.careerinnovation.com

Acknowledgements

This paper was prepared by Michael Moynagh (Senior Research Fellow) and Nilanthi Samaranayake (Researcher) on behalf of Ci, with support from Jonathan Winter, Prabhu Guptara and the **stars** team.

Thanks also to Jonathan Hyde of Risk Solutions, John Bray and Sara Braccheschi of Control Risks, Joseph F. Coates, Arjun Singh-Muchélle of United Nations. This research does not necessarily reflect their opinions but we are very grateful for their support.

What will happen to transnational crime?

Transnational crime refers to crime carried out by global networks across territorial borders. It includes money laundering, internet crime, people smuggling, the drug trade, counterfeiting and other forms of organised crime. Terrorism could be included, but is beyond the scope of this paper.

The story so far

A growing number of crime groups are centred in no one jurisdiction but operate in many – for at least three reasons.

- Globalisation has increased the opportunities for cross-border crime, as the volume of global transactions has risen. In 2005 the UN put the global narcotics trade at an estimated US$320 billion.[1]

- Weak states have created the conditions in which global crime can flourish. The collapse of the Soviet Union fuelled a big expansion of crime in much of Eastern Europe, and the effects are still being felt today.

- The internet is being used by global crime groups for fraud, theft, extortion schemes, money laundering, to rig gambling on online sites and to connect with hackers, who assist the crime groups with viruses and spyware.[2]

The expansion of transnational crime has encouraged global cooperation in response. Europol, for example, became fully operational in 1999 and coordinates cross-border policing and criminal investigations in the EU.

The UN Convention against Transnational Organised Crime came into force in 2003.

- It provides a common definition of organised crime.

- It obliges countries to establish money laundering, corruption and certain other activities as criminal offences.

- It offers 'what is potentially a world-wide framework for cooperation against organised crime.'[3]

---

1 *World Drug Report 2007,* United Nations, 2007, p. 170.

2 Phil Williams, 'Organized Crime and Cybercrime: Synergies, Trends and Responses', 13 August 2001, http://www.crime-research.org/library/Cybercrime.htm.

3 'The response to international crime', http://www.fco.gov.uk.

What will influence the next 20 years?

As the world recovers from the current recession, economic growth will increase volumes of traffic – whether people travelling through airports or the checking of credit card details. This will create new opportunities for criminals, who will find it easier to hide their illicit transactions amid all this 'noise'.

New opportunities

There will be many new opportunities for crime. In 2006, for instance, only half a million consumers had credit cards in China.[4] This figure will balloon as China's middle class grows to approaching 600 million by the 2020s.[5] Opportunities for credit card fraud will soar.

©iStockphoto.com/mevans

States with weak or non-existent governments will continue to create conditions in which global crime flourishes. Somalia saw 60 incidents of piracy off its coast in just the first three months of 2009.

A Ukrainian ship carrying arms was released only after pirates were paid US$3.2 million in cash. An international brigade of roughly 15 ships currently polices the Horn of Africa.[6]

In states with strong governments, corruption helps to blur the distinction between what is legal and moral, aiding transnational crime. UN Secretary-General Kofi Annan declared in 2004:

'It is now widely understood that corruption undermines economic performance, weakens democratic institutions and the rule of law, disrupts social order and destroys public trust, thus allowing organised crime, terrorism and other threats to human security to flourish.'[7]

A growing pool, worldwide, of unemployed young people will provide an expanding source of labour for organised criminals.

---

4 An estimate by Experian, the UK-based credit information company, *The Times*, 22 November 2006.

5 Chinese Academy of Social Science report, quoted in the *China Daily News*, 27 October 2004. The Academy's report expected 40% of China's 1.4 billion people in 2020 to be middle class. Middle class is defined as families with assets of roughly $18,000 to $36,000.

6 Mark Mazzetti And Sharon Otterman, "U.S. Captain Is Hostage of Pirates; Navy Ship Arrives," *The New York Times,* April 8, 2009

7 UN Office on Drugs and Crime, *Global Action Against Corruption. The Merida Papers,* UN, 2004, p. 1.

Global crime networks often sub-contract work to individuals on the edge of the legitimate economy. These people dispose of smuggled goods and provide other support to earn incomes not available from lawful jobs.

Dr Ifzal Ali, chief economist of the Asian Development Bank, has warned of a 'huge global oversupply of labour', particularly in China, India and Russia.

India's working-age population is expected to grow by 71 million between 2006 and 2011. Many could be unemployed and turn to the criminal economy.

New types of crime

The US government's National Intelligence Council has identified computer-based information as a 'key battlefield' of the future. This data is 'far more valuable and vulnerable' than physical systems. 'Cyber warfare' will be a growing threat.[8]

In a 2008 survey of security practitioners mainly in business, 44% reported incidents arising from insider abuse of networks.[9]

©iStockphoto.com/henkeimages

These incidents will become more numerous and take novel forms as employees accidentally put their organisations at risk – from careless employees who leave passwords out in the open, to IT managers who forget to install the latest security updates, to an employee who feels wronged and is out for vengeance.[10]

As now, some employees will knowingly collaborate with criminals or be coerced into doing so.

Existing crimes will take new forms – witness the innovative types of kidnapping that have recently emerged. In Latin America, for instance, express kidnapping involves taking victims on a tour of ATMs and instructing them to use their credit cards.[11]

---

8 *Mapping the Global Future 2020*, U.S. National Intelligence Council , 2004, p. 97 http://www.dni.gov/nic/NIC_globaltrend2020.html

9 Robert Richardson, "2008 CSI Computer Crime and Security Survey," Computer Security Institute http://www.gocsi.com/

10 Interview with Jonathan Hyde of Risk Solutions on 8 May 2009.

11 Control Risks, "Monthly Kidnap News," Issue 36, February 2009.

Who defines crime will be an issue. Global corporations will continue to press for international business standards.

As these are agreed, practices that were once common in parts of the world will become illegal. Stamping out these new crimes, as now, will not always be easy.

Better law enforcement

On the plus side, law enforcement agencies will tackle crime more effectively. Despite the history of poor collaboration, political pressure will force agencies to work more closely together, improving their effectiveness. Countries will gradually pool criminal records and knowledge of good practice.

Enforcement agencies will have certain advantages over organised crime. Lack of trust between criminal groups will limit the sharing of knowledge between them, while political bosses will press agencies to overcome problems of security and trust.

©iStockphoto.com/adroach

Likewise the banks, who are at the nexus of much transnational crime, and other companies will continue to collaborate more closely on crime.

Cooperation will be the key to success. If governments and companies fail to collaborate better than criminals, the future for this issue is bleak.

In addition, agencies will develop new techniques to match those of criminals. Once a crime has been solved, for example, agencies will more often analyse the sequence of events that led up to the crime, identifying steps to prevent a repetition in future.[12]

US defence spending increasingly focuses on terrorism. Huge sums will be invested in developing technologies that will also benefit the fight against global crime.

[12] Michael Levi & Mike Maguire, 'Reducing and preventing organised crime: An evidence-based critique', *Crime, Law & Social Change*, 41, 2004, p. 431.

Limits to law enforcement

But there will be limits to what law enforcement agencies can achieve. Success against crime in one context will displace it to another. Criminals may shift to other locations, find new targets or turn to other types of crime.[13]

'Target hardening' in the case of internet crime may encourage offenders to move to the drug trade or people smuggling, or to develop new types of online crime. The battle against crime can never be won, though much can be done to contain it.

What might be the implications?

Leaders will find that crime is near the top of their in-trays. One panel of experts rated commercial espionage by corporate spies as the biggest upcoming threat to business from internet crime.[14]

As security is tightened, criminals may resort to more extreme measures such as extortion – 'We'll bribe a local official to close your supplier's factory in Asia, if you don't help us.'

Prevention will include treating employees well so that they don't have a reason to act maliciously. Ensuring that employees have access only to information they need to know will limit the opportunity for them to pass on information to criminals.

Small firms should beware. As larger organisations use their considerable resources to improve security, criminals may turn to smaller companies that are less well protected.

Knowledge-based assets will be at particular risk. The shift to a knowledge economy will mean that more and more organisations will base their competitive advantage on unique databases of information and on specialist expertise.

In some parts of the world, kidnapping may become a form of corporate espionage. Knowledge-rich staff may need protecting from criminal gangs seeking to extract confidential information from them.

Health systems that centralise patient records will face increased risk from hackers, wanting to access and sell the records of public

---

13 Russell G. Smith, Nicholas Wolanin & Glenn Worthington, 'e-Crime Solutions and Crime Displacement', *Trends & Issues in Crime and CriminalJustice*, 243, Australian Institute of Criminology, January 2003.

14 Sheridan Morris, 'The future of netcrime now: Part 1 – threats and challenges', Home Office Online Report 62/04, 2004, p. 16.

figures. Corporations will face similar threats to their customer records.

Global crime will push up the costs of legitimate business. Organisations will have to spend more on security arrangements. In a 2005 survey, 56% of firms in Saudi Arabia planned to introduce iris scanning and fingerprint recognition in their offices.[15]

If piracy spreads, the cost of shipping will rise. As rare metals become increasingly important in parts of manufacturing, such as electric cars, criminal threats to the security of supply may be a growing problem.

But it won't all be bad news. Increased shopping online may reduce the amount of theft retailers experience in their stores. Will online be cheaper than in-store security?

Global crime will encourage companies to cooperate on security. Banks, for example, will not only pool information. They may pool resources to pay hackers and other criminals to come over to their side and enhance their security arrangements, instead of attacking them.

Banks in particular may turn their security expertise into a new source of income. They may sell their specialist knowledge to other organisations wanting to protect themselves.

Companies may exchange technical knowledge and jointly develop new techniques, but remain reluctant to share information about security breaches lest details become public and undermine confidence.

If this reluctance extends to law enforcement agencies, governments may increasingly wipe their hands of business-related crime. They will leave security to the companies themselves, pushing up business costs.

Will firms eventually create law enforcement networks that are not publicly accountable – private versions of what the state does? And if so, will this give rise to mounting public concern?

Work could be more controlled and less attractive. Processes and technologies will be developed to increase security at work, especially internet security.

In some cases, even the most innocuous information will have to be looked at carefully. Twitter and other social networks will allow criminals and competitors to piece together disparate bits of

[15] Eamonn Kelly, *Powerful Times,* New Jersey: Wharton School Publishing, 2006, pp. 24-31.

information to discover developments that a company would rather they didn't know.

Mapping workers' travel and locations might reveal that their employer was in secret negotiations with a particular company or developing a presence in a certain country.

Might certain employees be instructed not to twitter while they were travelling or disclose their movements on other social networking sites? Such measures could leave staff feeling increasingly regulated, reducing work satisfaction.

Or will organisations find alternative, more work-enriching approaches? These might include steps to increases trust and localise risk – a breach of security would impact only those immediately responsible and their co-workers.

Of particular importance, security measures could make it harder for employees to share information, stifling the generation of knowledge that increasingly will be critical to success.

Solving this dilemma will bring organisations considerable rewards. It may have surprising effects on how people are organised at work. Will it accelerate the adoption of decentralised models?