eSeminar Primer

Centre for Security Governance

No. 3 | July 2014

*The Centre for Security Governance eSeminars bring together leading security sector reform experts to discuss a range of SSR-related issues and cases on a quarterly basis.*

# New Frontiers in Security Sector Reform: Countering Technology-Driven Threats

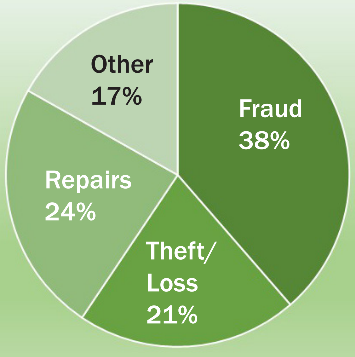
Cyberspace – in an economic, political, and social sense – is a central part of many people's contemporary existence. Over US$200 billion worth of products are bought online annually,[1] while businesses often have a substantial online presence. Governments recognize that cyberspace allow them to more efficiently deliver public services, resulting in more government documents being requested or renewed online and greater departmental accessibility.[2] Finally the rise of social media, most notably Facebook and Twitter, has connected tens of millions of people and created new avenues of communication and forms of interaction.[3]

While the promise of cyberspace is great, its potential can be undermined by criminal organizations seeking to find and exploit software and hardware loopholes for illicit gains. Cybercrime encompasses a broad spectrum of activities from intellectual property and identity theft to industrial espionage and attacks on server infrastructure.[4] The economic cost of cybercrime is huge, estimated at US$113 billion last year – a number that encompasses fraud, theft or loss, repairs, and other costs (see Figure 1). However the impact of cybercrime is not simply financial; it can cause service and employment disruptions, damage to corporate brands and reputation, inconvenience to consumers, potential delays in fulfilling business obligations, and consequent loss of trade and competitiveness.

Surprisingly, the security sector reform (SSR) literature has largely ignored this issue. Building cybersecurity defences, governance insti-

Centre for Security Governance

**Figure 1: Global Price Tag of Consumer Cybercrime, 2013 (US$113 BN) – Breakdown**



Adapted from: Norton, *2013 Norton Report* (Toronto: Symantec Corporation, 2013).

tutions, and legal instruments in developing countries to counter and mitigate technology-driven threats like cybercrime has not figured prominently in the plans of international donors and aid agencies. Indeed, with a few exceptions, cybersecurity has rarely been explored by SSR scholars and practitioners,  despite the fact that the ability of developing countries to adapt and respond to emerging cybersecurity threats – especially cybercrime – will have a huge impact on how individuals, businesses, and states communicate and engage with one another.

Developing countries account for a small, but growing portion of cybercrime activity (See Figure 2). This trend is likely to continue with the dramatic rise of internet usage in the developing world from only 8 percent in 2005 to 31 percent in 2013.[5] Developing countries will exert an ever larger impact on the nature of

## About the eSeminar Series

The Centre for Security Governance eSeminars are a series of virtual meetings that bring together experts and practitioners from around the world to discuss security sector reform (SSR) and related themes, issues, and case studies. The eSeminars are open to the public, and includes three key components: the eSeminar Primer, eSeminar Summary, and eSeminar Videos. For information on upcoming eSeminars, please visit http://www.secgovcentre.org/events.

Series Editor: Mark Sedra
Report Author: Matthew Morgan

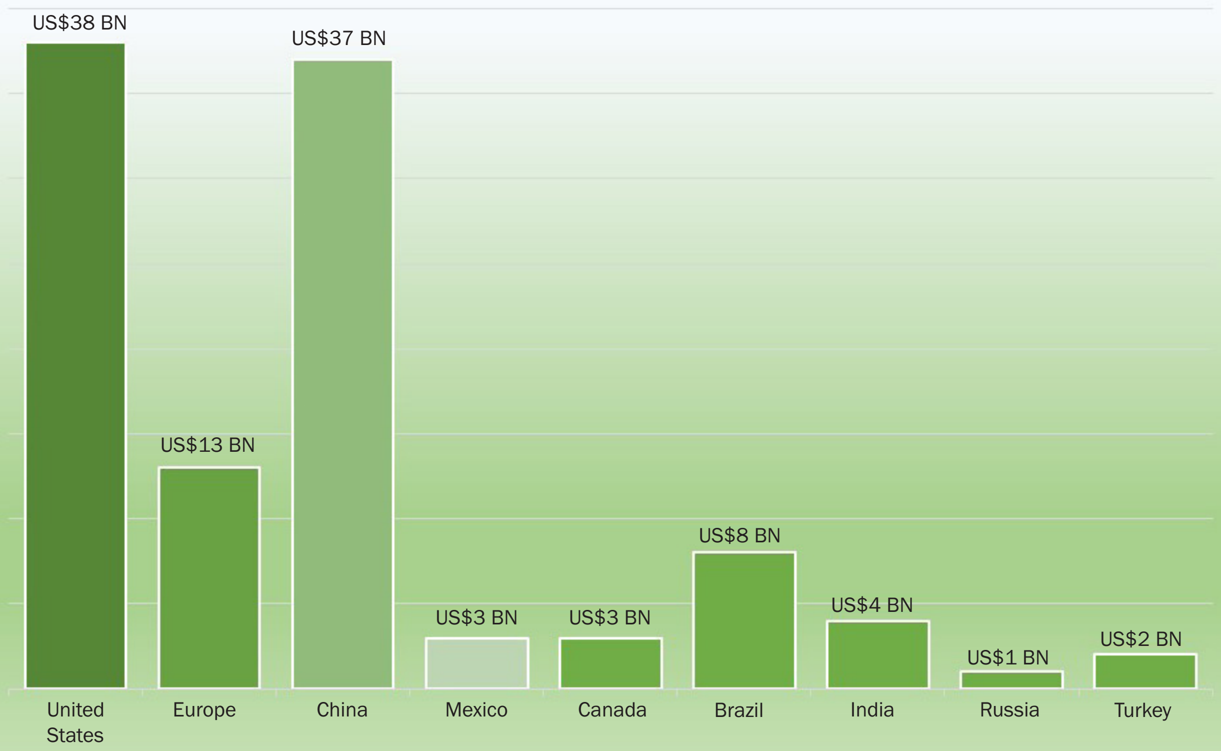
## About the CSG

The Centre for Security Governance is a non-profit, non-partisan think tank dedicated to the study of security transitions in fragile, failed and conflict-affected states, a process also known as security sector reform. A registered charity based in Kitchener, Canada, the CSG maintains a global network of research fellows from a variety of backgrounds, including practitioners, research analysts and academics, and partner organizations from the public and private sector engaged in SSR.

Centre for Security Governance
Tel: +1 226 241 8744
Email: info@secgovcentre.org
Web: www.secgovcentre.org
SSR/RC: www.ssrresourcecentre.org

The opinions expressed in this paper are those of the author(s) and do not necessarily reflect the views of The Centre for Security Governance or its Board of Directors. This work was carried out with the support of the Centre for Security Governance, Kitchener, Ontario, Canada (www.secgovcentre.org). This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this license, visit (www.creativecommons.org/licenses/by-nc-nd/3.0/).

**Figure 2: Global Price Tag of Consumer Cybercrime, 2013 – By Country**



Adapted from: Norton, *2013 Norton Report* (Toronto: Symantec Corporation, 2013).

cybersecurity, both in terms of threats and in the responses to them.

Kavanagh, Maurer, and Tikk-Ringas point out that governments are only just starting to get serious about cybersecurity in the developing world. As they note, donors are starting to offer support in key areas, including "reform and harmonization of legislation; countering crime and terrorism and the identification and sharing of good practices."[7] It is a potentially major oversight to ignore this topic, given that an open and safe Internet is fundamental both to ensuring and protecting political freedom and as an engine of future global economic growth. Yet private and public SSR stakeholders have only recently begun to formulate strategies, conduct research, and distribute funding to support cybersecurity initiatives in developing countries.

Cybersecurity is only now being considered a potential part of the SSR framework. The majority of organizations that deal with cybersecurity in an SSR context are either less than five years old or are older organizations that have established branches to examine this issue. Private and public stakeholders are still in the early stages of formulating strategies, conducting research, and distributing funding to support cybersecurity initiatives within an SSR framework. Kavanagh argues that this delayed response stems from the difficulty that development actors historically have had in confronting traditional criminal issues: "The development community has been slow to integrate an 'organized crime-sensitive' approach to its programming, despite a growing acknowledgement that organized crime can have important impacts on governance and development, and that organized crime and politics frequently interact to provoke varying degrees of instability."[8]

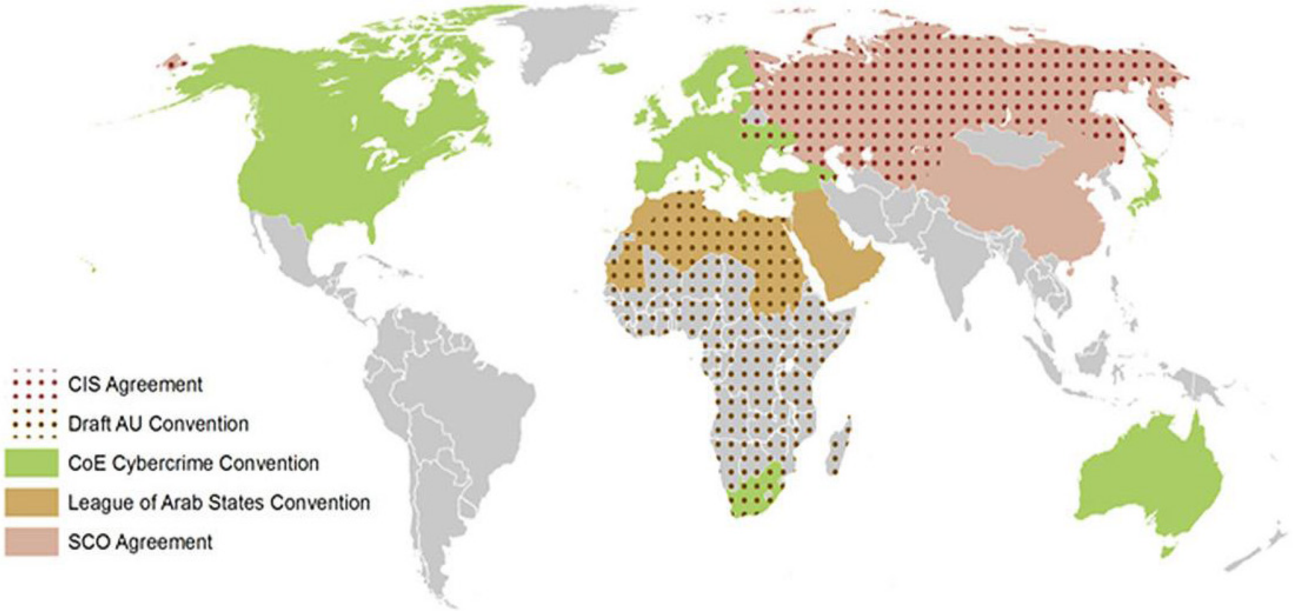
**Table 1: International Organizations and Partnerships Providing Cybercrime Assistance**

| Name | Year Founded | Description |
|---|---|---|
| International Telecommunications Union | 1865 | A UN organization, the largest dealing with cybercrime and cyber governance issues today. Focuses on capacity-building in developing countries. |
| NATO – Science for Peace and Security Programme | 1958 | Tasked with dealing with cybersecurity issues in 2004. Runs a range of cyber-security training programs in partner states. |
| Organization of American States – Cyber Security Program | 2004 | Seeks to develop and codify common legislation and procedural measure in regards to cybercrime among its members |
| International Cyber Security Protection Alliance | 2011 | A partnership between Western countries, private corporations, and developing states, the ICSPA is designed to channel funding and expertise in order to reduce cybercrime in developing countries |
| International Multilateral Partnership Against Cyber-Threats | 2011 | The cybersecurity executing arm of the ITU. Bills itself as a CDC for cybersecurity, tracing in real time emerging cyber threats. |
| Interpol Global Complex for Innovation | 2014 | A new branch of Interpol that will be tasked with developing new techniques to prevent and combat cybercrime. |

With this in mind, it should not be surprising that a rapidly altering technological, geopolitical, and economic environment has quickly outpaced SSR stakeholders, forcing them to catch up and to create new governance frameworks and enforcement mechanisms in response. The number of institutions that place cybercrime as a central concern is small but growing (see Table 1), as states and international bodies begin to take seriously the threat posed by increasingly organized cyber criminals.

Cybercrime is a highly organized and profitable activity. The United Nations estimates that upwards of 80 percent of cybercrime originates in some form of organized activity.[10] Yet no uni-

Figure 3: International and Regional Instruments that Govern the Response to Cybercrime



Source: Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas, *Baseline Review ICT-Related Processes & Events: Implications for International and Regional Security* (Geneva: ICT4Peace Foundation, 2014).

fied legal or political instruments exist to police and deter those who engage in these criminal activities. Instead a plethora of different regulatory instruments and regimes exist (see Figure 3), with many areas of the world lacking any comprehensive agreement that penalizes cybercrime.

A comprehensive and global approach that connects international organizations and aid groups along with donor countries and developing states is sorely needed in the area of cybersecurity. Tentative steps in this direction are being taken with the increasing involvement of developing countries in discussions on how to best deal with cybercrime, from supporting certain cybercrime-focused police reforms to ensuring developing countries have the institutional legislative and justice structures in place to deal with cyber threats. This is a positive advancement. At the very least, it is an indication that governance and legal frameworks around cybersecurity issues are continuing to expand and mature. However, there is a long way left to go towards formulating a substantial SSR strategy to combat cybercrime.

## Notes

[1] Stu Woo, “Online-Retail Spending at $200 Billion Annually and Growing,” *Wall Street Journal*, 27 February 2012.

[2] United Kingdom, Cabinet Office, “Government ICT Stratregy” (Cabinet Office, London, 2013); Joseph Andersen and Daniel Coffey, “US ICT R&D Policy Report: The United States: ICT Leader or Laggard?” Telecommunications Industy Association Innovation White Paper.

[3] Further information on the impact of cyberspace on social interaction can be found in Barry Wellman, *Networked: The New Social Operating System* (Cambridge: MIT Press, 2012).

[4] The United Nations Office on Drugs and Crime provides an overview of different forms of cybercrime and their economic impact. See United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013).

[5] Two exceptions to this overall dearth of analysis are M. Gercke, “Understanding Cybercrime: A Guide for Developing Countries,” International Telecommunications Union, 2011; and Zeinab Shalhoub, and Sheikha Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies* (Worchester: Edward Elgar, 2010.)

[6] International Telecommunications Union, *Trends in Telecommunication Reform 2013* (Geneva: International Telecommunications Union, 2013), p. 2.

[7] Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas, *Baseline Review ICT-Related Processes & Events: Implications for International and Regional Security* (Geneva: ICT4Peace Foundation, 2014), pp. 43-44.

[8] Camino Kavanagh, *Getting Smart and Scaling Up: Responding to the Impact of Cybercrime in Developing Countries* (New York: Center for International Cooperation, 2013), p. 7.

[9] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, p. xvii.