Financial Fraud, Technology Disruption, and Cyber-Governance

Yves Ekoué Amaïzo
Director Afrocentricity Think Tank, Austria

INTRODUCTION

A large number of cyber-activities disruptions have economic and financial consequences. Numbers of those disruptions turn out to be economic cyberfraud or cybercrimes, defined as a breach of common and criminal law implemented with digital technologies and networks. They bring into being emerging threats on human progress and social cohesion. Mainly for security reasons, unilateral decisions from States are limiting participative approaches with major cyberstakeholders. The objective of this article is to advocate for multi-stakeholders cybergovernance for a free circulation of knowledge. It may require a neutralization of glocal (local and global) cybertreats and unnecessary cyberinformation snatching often hidden behind security justifications.

BACKGROUND

Opportunity and Threats of Cyberknowledge

Information, science and technology (IST) is an interdisciplinary field of knowledge expertise. With the growing connectivity, cybervulnerability and cyberthreats depend on a secured governance of the World Wide Web infrastructure and the reliability of related technologies otherwise changing threats into opportunities becomes impossible. Mastering the available worldwide knowledge and generating value added information and wealth turns are a competitive issue. Besides the ethical requirements, IST is nowadays highly dependent on the ability to access, produce, store, communicate and manage data, information and knowledge. In an interdependent world economy wired with fast evolving cybersystems with disruptive technologies and cloud networks, IST recurrently faced pervasive and insidious activities on cyberspace. Often, States security has a priority over people's privacy or organizations' confidentiality. In recent times, a new frontier of information transparency has emerged with the revelations of diplomatic cables intercepted and published by WikiLeaks. Surprisingly, States which were supposed to guaranty the cybersecurity are part of this controversial issue[1].

Issues and Challenges

The sustainability of private and public Internet Safety is a major world challenge. The prevention and adoption of secured digital technologies require a participative system of regulation and control by individuals as well as organizations including States. Failing to master this, Internet governance could yield in high costs in terms of direct liabilities such as unexpected burdens due to technology, network and market disruptions, negative externalities of unsafe and insecure web. It could result in monetary and indirect liabilities such as reputation (Amaïzo, 2012).

Problems

Regulation is required for an efficient cybersecurity framework. *Deregulation* as an alternative is not an option as the drain on individuals and organizations' resources might be economically unsustainable. Yet, the principle of disrupting cyberactivities is perceived and sometimes rewarded as a competitive profitability business. Forged and malicious technology disruption resulting in a cyberinformation snatching or a

DOI: 10.4018/978-1-4666-5888-2.ch146

cybermoney grabbing appears as a *'normal'* trading business especially in a profitable market segment of Electronic (E) commerce and E-marketing.

Controversies

From a formal law (common and criminal) viewpoint, making business on an unsecure and unpredictable Internet system could be perceived and associated with financial fraud, crime or terrorism. The lack of harmonization between several jurisdictional law enforcement entities and legal tax heaven territories is reinforcing this perception. The main controversy consists in the trivialization of cyberpreemptive actions and the potential interference of most influential and technologically advanced actors.

Forward Guidance Proposal

One of the forward guidance proposals to this multi-dilemma problem is to reengineer partnership surveillance on cyberissues. Cybersafety is crucial for trade, business and innovation. As privacy, freedom, justice and equal rights to free flows of information, science, technology and knowledge are essential for the building of a society of trust, cyberactivities must be safe and transparent. The most technologically advanced cyberactors should be prevented to engage in global cyberspying of others or use freely posted private information for their direct interests. Such a behavior is not sustainable and could even become contra-productive if new technologically advanced actors emerge and retaliate.

Strategic Orientations

Seven interdependent strategic orientations are suggested. Firstly, with the rise of malicious cyberactivities, destructive creation behavior and culture should be discouraged. Subsequently, economic cyber fraud and crime should be traced, stopped and cyberwrongdoers prosecuted. Secondly, a broader definition of financial fraud and crime is required and should include financial terrorism as well as cybertechnology disrupters. Thirdly, money incentives could be used to convert former fraudsters or criminals to comply with ethics. It could be less effective in weak law enforcement economies as compared to digital edge economies. Fourthly, it is of utmost importance that cyberactors and stakeholders are not marginalized and become a problem. They should be part of the solution to safe cyberenvironment. Hence, cyberwrongdoers should not be empowered to leverage on cyberinstruments. Fifthly, combating illegal cyberactivities require the combination of both formal and informal regulatory framework. Restricting access to Internet for all cannot be considered as an alternative in cyberspace (The White House, 2011). Sixthly, one of the challenges of the 21st century is to increase collective security on cyberspace. It might require the establishment of a Supreme Court on cybersecurity. Seventhly, solutions to neutralize unlawful and illicit digital intrusions are complex. A comprehensive cyberaccountability is required.

MAIN FOCUS OF THE ARTICLE

Economic Cybercrime and *Destructive Creation* Culture

According to the *Symantec Global Internet Security Threat Report* of 2012, the World has experienced an exponential growth from 1 billion in 2006 to 5.5 billion malicious attacks in 2011 with 81% upsurge between 2010 and 2011. At least 403 million unique variants of malware, 41% increase in 2011 as compared to 2010, were blocked. 42% of mailboxes targeted by cyberfraudsters or criminals in 2011 belonged to executives, senior managers and knowledge workers. 50% of targeted attacks focused on small and medium-sized businesses over 200 countries. Mobile phones as well as social networks becomes new targets for cybercriminals who are exploiting cyberinfrastructure vulnerabilities as malware is by 97% hosted on a legitimate website (Symantec, 2012). With an impressive increase of 29% of malicious websites between 2009 and 2010, and the long-lasting 2008 financial crisis, any technology and cyberdisruption affecting the financial sector will negatively impact States, business and individuals.

Financial fraud and crime are acknowledged as an emerging risk in an increasing open world trade of goods, services, finance, people, technology, data, information and knowledge. This economic-cybercrime is controlled by organized cutting-edge entities. It is