CIFA-BC | COUNTER ILLICIT FINANCE ALLIANCE BRITISH COLUMBIA

AML Review

Volume 2, Issue 3 - June 2025

Special Issue: Cyber-Dependent and Cyber-Enabled Financial Crime

About this Issue

This Special Topics Bulletin focuses on cyber-dependent and cyber-enabled financial crime.

Accessing AML Review Disseminations

Copies of individual articles contained within AML Review will be stored on GC Collab. If you are unable to access an article, please email CIFA-BC@rcmp-grc.gc.ca.

Classification Level

Classification Level: Unrestricted - Open for public sharing

This Bulletin is intended for internal use within CIFA-BC partner agencies/organizations and can be shared with trusted individuals and third-parties.

INTRODUCTION

Welcome to *AML Review,* your resource for staying up to date with developments in anti-money laundering (AML) efforts, including scholarly outputs, government reports, and case law.

This issue of *AML Review* focuses on cyber-dependent and cyber-enabled financial crime. Cyber-dependent financial crime refers to illegal financial activities that can only be committed using digital technologies and online systems. This includes hacking, ransomware attacks, phishing, and malware. Cyber-enabled financial crime refers to financial crimes that use digital technology, such as the internet, mobile devices, and computer networks, to facilitate, enhance, or conceal financial crime. For instance, cybercriminals may use computer systems or online financial services to conceal the source of illegitimate funds or commit fraud. Cyber-dependent and cyber-enabled financial crime are desirable to criminals given the speed, scale, and anonymity with which they can be carried out. Offenders can exploit technological vulnerabilities from anywhere in the world, often operating across jurisdictions. As financial systems become increasingly digitized, the risk of exploitation rises, placing pressure on law enforcement, financial institutions, regulatory bodies, and other stakeholders to adapt.

Understanding cyber-dependent and cyber-enabled financial crime are critically important because they threaten not only economic security, but also trust in financial systems. Furthermore, they undermine national and international stability. Cyber-enabled financial crime is closely linked to money laundering, as criminals often use computer systems and online financial services to launder money. Cyber-dependent crime generates illicit profits, which are then laundered by cybercriminals via cyber-enabled crime to disguise the origin of these funds and integrate them into the legitimate economy.

The goal of this special issue is to explore the methods and evolving trends of cyber-dependent and cyber-enabled financial crime and highlight evidence-based strategies for prevention, detection, and response. This special issue features four academic articles. First, is an article by Dupont (2024) that provides guidance for addressing cybercrime using an ecological systems framework. Second, is an article by Loggen and colleagues (2024) which presents the findings of a systematic narrative review on the pathways into, desistance from, and risk factors related to financial cybercrime. Third, is an article by Peersman and colleagues (2022), which presents the motivations and characteristics of those involved in cybercrime using data collected from practitioners working in law enforcement in the cyber crime field. Fourth, is an article by Wronka (2022) that examines how illegally obtained funds are laundered through online platforms using data collected from prevention experts, compliance, officers, and convicted cybercriminals.

Also included in this special issue is a Financial Action Task Force (2023) report that analyses how cyber-enabled fraud has evolved, how criminals may exploit vulnerabilities in new technologies, successful and recommended strategies for addressing cyber-enabled fraud, and risk indicators and controls to detect and prevent cyber-enabled fraud and related money laundering.

To assist readers with locating full copies of the articles featured in this issue, going forward each issue of *AML Review* will include hyperlinks to where an open-source copy of the dissemination can be located.

We hope that *AML Review* will continue to be a valuable resource for you to develop your expertise in AML. If you have an idea for a future bulletin or have materials you would like to share, please contact CIFA-BC@rcmp-grc.gc.ca.

Sincerely,

Dr. Catherine Shaffer-McCuish
Editor, *AML Review*
Counter Illicit Finance Alliance of British Columbia Intelligence Hub

INCLUDED DISSEMINATIONS

Academic Articles

Dupont, B. (2024). The governance of cybercrime: An ecological approach. *Canadian Journal of Criminology and Criminal Justice*, *66*, 1-23.

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, *52*, 105858.

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*. University of Bristol Cyber Security Group.

Wronka, C. (2022). "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*, 330-344.

Government Reports

Financial Action Task Force (2023). *Illicit financial flows from cyber-enabled fraud*. FATF.

ACADEMIC ARTICLES

Project and Scholarly Work

Dupont, B. (2024). The governance of cybercrime: An ecological approach. *Canadian Journal of Criminology and Criminal Justice*, *66*, 1-23.

Abstract

Cybercrime is now the most common form of crime in Canada and causes significant financial and psychological harm. The criminal justice system struggles to address cybercrime due to its complexity, scale, and global nature. Criminologists are also challenged to think about cybercrime beyond established theoretical frameworks. An interdisciplinary approach is required to understand this phenomenon and enable us to craft effective policies. The discipline of ecology can provide valuable insights and a practical integrative framework through the concepts of community, interaction, and emergent effects. First, a high-level outline is provided of how the cybercrime ecosystem can be analyzed using basic ecological concepts and principles. This framework is then applied to the security community, showing how it is populated with a diversity of organizational and institutional entities that can be enabled or compelled to act in ways that enhance online security through a broad set of regulatory strategies. Finally, three innovative configurations that take advantage of this regulatory pluralism and novel forms of collaboration are described to illustrate how alternatives can be implemented to mitigate the negative impacts of cybercrime with promising outcomes.

Project and Scholarly Work

Loggen, J., Moneva, A., & Leufeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review, 52*, 105858.

Abstract

Financial-economic cyber-enabled crime (hereinafter: financial cybercrime) has increased dramatically over the past years. However, research on financial cybercrime is still underdeveloped and highly heterogeneous, especially regarding the processes of initiation to and desistance from crime. This paper synthesizes existing knowledge on pathways into, desistance from, and risk factors related to financial cybercrime, and identifies research gaps. Adhering to PRISMA-ScR guidelines, the authors executed a systematic search and identified 37 eligible documents published as of February 2022, indicating two initiation points into financial cybercrime: involvement in traditional crime, and experiencing strain. Through social learning, individuals then learn the necessary skills and knowledge and engage in financial cybercrime, after which the decision to desist is influenced by a cost-benefit analysis, the use of neutralization techniques, and maturing. As for risk factors, the authors identified 33, with being male, unemployed, having low self-control and deviant peers, and wanting to earn money quickly being of potential importance. Regarding research gaps, there is a dearth of research related to the initiation and desistance processes of financial cybercrime, and the identified studies lacked a robust research designs, with 76 percent being of low or medium quality. More quality research is needed to address these issues.

Project and Scholarly Work

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*. University of Bristol Cyber Security Group.

Abstract

Cyber offences, such as hacking, malware creation and distribution, and online fraud, present a substantial threat to organizations attempting to safeguard their data and information. By understanding the evolving characteristics and motivations of individuals involved in these activities, and the threats that they may pose, cyber security practitioners will be better placed to understand and assess current threats to their systems and the range of socio-technical mitigations that may best reduce these. The reported work-in-progress aims to explore the extent to which findings from prior academic literature regarding the characteristics and motivations of offenders engaging in financially-motivated, cyber-dependent crime are supported by the contemporary experiences and perspectives of practitioners currently working in the cyber crime field. A targeted, online survey was developed consisting of both closed and open-ended questions relating to current cyber threats and the characteristics and motivations of offenders engaged in these activities. Sixteen practitioners working in law enforcement-related domains in the cyber crime field completed the survey, providing a combination of qualitative and quantitative data for analysis.

Project and Scholarly Work

Wronka, C. (2022). "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*, 330-344.

Abstract

Purpose: This study aims to illustrate and determine how illegally obtained funds are laundered through online platforms and companies in different economic sectors in the digital age. Design/methodology/approach: A qualitative analysis approach using purpose sampling methods, including 21 semi-structured interviews with prevention experts, compliance officers and convicted cybercriminals, resulted in the determination of concrete money-laundering methods involving the employment of online platforms provided by companies and institutions in different economic sectors. Findings: The current study focuses on various companies in different economic segments that mitigate cyber laundering and the anti-money laundering measures that can be adopted. Therefore, this paper provides a detailed discussion and analysis on how money launderers avoid being detected. Both preventive and criminal perspectives are taken into consideration.

Government Reports

Report

Financial Action Task Force (2023). *Illicit financial flows from cyber-enabled fraud.* FATF.

Abstract

Cyber-enabled fraud is a major transnational organised crime that has grown exponentially in recent years, both in volume of frauds reported and their global spread. Such crimes can have a devastating impact on individuals, organisations, and economies worldwide, causing significant financial losses and eroding trust in digital systems. The transnational nature of this crime, with proceeds of cyber-enabled fraud often rapidly transferred to different jurisdictions, makes this a global concern.

As digital innovation continues to advance, so will the sophistication and scale of cyber-enabled fraud, if left unchecked. The FATF, in partnership with the Egmont Group and INTERPOL, analysed how the cyber-enabled fraud landscape has evolved, its links to other crimes and how criminals may exploit vulnerabilities in new technologies. The report highlights examples of national operational responses and strategies that have proven successful in tackling cyber-enabled fraud. This includes the need to break down siloes and accelerate and enhance collaboration across

various sectors and on both the domestic and international levels.

It is essential that countries work together and take action to stop the escalating threat of cyber-enabled fraud. The report identifies three priority areas in which jurisdictions should act to tackle this crime and related laundering more effectively: enhancing domestic co-ordination across the public and private sectors, supporting multi-lateral international collaboration, and strengthening detection and prevention by promoting awareness and vigilance and facilitating reporting of such crimes.

The report also identifies risk indicators and useful anti-fraud requirements and controls, that may help public and private sector entities detect and prevent cyber-enabled fraud and related money laundering.