S. LYEONOV, T. VASYLIEVA & H. FILATOVA

Financial Fraud and Cybercrime in Wartime:

An Overview of the Scientific Landscape and Insights from Countries Engaged in Military Conflict

FINANCIAL FRAUD AND CYBERCRIME IN WARTIME: AN OVERVIEW OF THE SCIENTIFIC LANDSCAPE AND INSIGHTS FROM COUNTRIES ENGAGED IN MILITARY CONFLICT

Monograph

Dr Prof Serhiy LYEONOV
Dr Prof Tatiana VASYLIEVA
Ph D Hanna FILATOVA

The Academic Research and Publishing UG (i. G.)
(AR&P, Hamburg, Germany), 2024

Reviewers:

PhD Assoc. Prof. Maryna Brychko
Blekinge Institute of Technology, Sweden

PhD Assoc. Prof. Yuliia Serpeninova
University of Economics in Bratislava, Slovakia

Dr Assoc. Prof. Maryna Utkina
University of Warwick Law School, UK

This publication has been approved by the Academic Research and Publishing UG (i. G.) (AR&P, Hamburg, Germany), to be issued as a scientific monograph.

Suggested citation:

Lyeonov, S., Vasylieva, T. & Filatova, H. (2024). Financial Fraud and Cybercrime in Wartime: An Overview of the Scientific Landscape and Insights from Countries Engaged in Military Conflict. The Academic Research and Publishing UG (i. G.), Hamburg, Germany, 187 p. doi: 10.61093/978-3-911748-02-5/2024

Publishing House: Academic Research and Publishing UG (i. G.)
https://armgpublishing.com/

Hamburg, Germany, 2024

ISBN 978-3-911748-02-5

DOI: 10.61093/978-3-911748-02-5/2024

First edition, 2024

To read this book's free, open-access version online, scan this QR code with your mobile device:

CONTENTS

CHAPTER 3: Cybersecurity and digital transformation of the war and post-war economy: fighting cybercrime, financial fraud, corruption and the shadow sector

INTRODUCTION

In the modern world, which is rapidly changing under the influence of globalisation, digitalisation and geopolitical challenges, financial stability is becoming a key condition for the sustainable development of countries and regions. However, this process is becoming more complicated due to the rise of financial crimes, including fraud and cybercrime. In the context of armed conflicts, such as the war in Ukraine, these threats become particularly relevant, creating additional risks to national and regional financial security. In such periods, organised criminal groups and individual criminals intensify their activities, using social and economic instability to implement fraudulent schemes and cybercrime.

The rapid development of digital technologies and information systems has greatly facilitated access to financial resources, but at the same time created new opportunities for financial crime. Cybercrime, as one of the most common forms of financial crime, includes data theft, payment system fraud, money laundering through cryptocurrencies and many other forms of illegal activity. Armed conflicts add a new dimension to this problem, as they disrupt the functioning of state institutions, reduce control and accountability, create new

schemes for illicit trafficking, and increase the social vulnerability of citizens.

The scientific literature has already covered a significant amount of research on the analysis of financial crimes in stable conditions, but much less attention is paid to the study of this issue in the context of a geopolitical crisis or military operations. Analysing changes in the behaviour of criminals, identifying new fraud schemes and assessing the effectiveness of existing countermeasures in times of war remain important issues that require detailed study.

The experience of countries that have experienced military conflicts, such as Syria, Iraq or Yugoslavia, shows that war creates favourable conditions for financial crime. For example, the destruction of state institutions, chaos in the banking system and imperfect regulatory mechanisms contribute to the emergence of new schemes for illicit enrichment. At the same time, such situations require immediate intervention by the international community, governments and law enforcement agencies to develop effective strategies to combat these phenomena.

The war in Ukraine, which has been ongoing since 2014 and escalated in 2022, has also created favourable conditions for the intensification of financial crime. In particular, cases of misappropriation of humanitarian aid, fraud with state

payments, and large-scale money laundering operations have become widespread.

In addition, digital attacks on government agencies and businesses have increased significantly, which demonstrates the need for a systematic approach to protecting the digital space in times of war.

The study of financial crimes in the context of military conflicts allows not only to identify new threats but also to develop more effective strategies to prevent them. For example, analysing cybercrime in times of geopolitical instability can provide valuable information for strengthening digital infrastructure, improving legislative frameworks, and enhancing international cooperation. Furthermore, understanding the behaviour of criminals in a crisis helps to create adaptive risk management models that take into account the specifics of wartime.

The main purpose of this monograph is to analyse financial crimes, in particular fraud and cybercrime, in the context of armed conflict, using the example of Ukraine and other countries that have been in a state of war. The monograph will examine the main fraud schemes, methods of their implementation, as well as countermeasures used by state and non-state institutions. Particular attention is paid to the analysis

of cybercrime, which is becoming one of the biggest threats to financial stability in the digitalised world.

The monograph aims to achieve the following key objectives:

– to summarise the current scientific landscape on financial crimes in wartime, including fraud, money laundering, corruption, the shadow economy and organised financial crime;

– to systematise existing financial crime schemes and methods of their implementation during armed conflicts, including analysis of the specifics for Ukraine and other countries affected by military operations;

– to identify the dominant research areas in the global scientific community, including key thematic clusters, cross-sectoral links, and the dynamics of changes in the use of dominant keywords;

– cluster scientific achievements by geographical and institutional origin, identify research leaders, educational and scientific institutions that have made the greatest contribution to the development of this topic;

– to analyse the dynamics of changes in scientific interests, the chronology of changes in case studies and the main stages of development of scientific discourse in the field of financial crime in the context of war;

– to develop practical recommendations for improving public policy, international cooperation and educational initiatives to effectively combat financial crime in times of crisis.

The research is based on an interdisciplinary approach that combines elements of economics, law, information technology and sociology. It uses bibliometric analysis, trend analysis, and modern machine learning tools to identify key patterns and trends in financial crime. In addition, the monograph will compare the experience of Ukraine and other countries in the fight against financial crime, which will allow us to identify the most effective practices and develop recommendations for improving national policy in this area.

The results of this study are of great practical importance. They can be used to increase the effectiveness of government programmes to combat financial crime, improve legislation, and develop educational initiatives aimed at raising public awareness of financial risks. In addition, the data obtained may serve as a basis for the development of international standards for combating financial crime in times of crisis.

Thus, this monograph not only fills a critical gap in the literature on the analysis of financial crimes in times of military conflict, but also contributes to the development of new approaches to financial security. Based on the results of the

study, the authors aim to contribute to the understanding of the complex interrelationships between financial crime, digital technologies, and armed conflicts, as well as to provide practical recommendations for minimizing risks in the future.

The authors are responsible for the originality of the text of the materials provided, the accuracy of the facts, quotations, statistics, proper names, geographical names and other information, as well as for the fact that the materials do not contain data that are not subject to open publication. DeepL was employed for English language proofreading.

CHAPTER 1: THE PREVENTION OF FINANCIAL FRAUD, MONEY LAUNDERING, CORRUPTION, SHADOW ECONOMY AND THE ORGANISED FINANCIAL CRIME IN WARTIME: AN OVERVIEW OF THE SCIENTIFIC LANDSCAPE AND INSIGHTS FROM COUNTRIES ENGAGED IN MILITARY CONFLICT

1.1 Schemes of the financial fraud, money laundering, corruption, shadow economy and the organised financial crime in wartime[1]

Wartime conditions create a complex environment of socio-economic instability and institutional vulnerability, leading to an upsurge in financial crimes. These crimes exploit gaps in governance, lack of oversight, and emergency financial flows linked to humanitarian aid, defense spending, and reconstruction. Understanding the mechanisms and dynamics of financial fraud, money laundering, corruption, shadow economy activities, and organized financial crime during wartime is essential for designing effective countermeasures and fostering post-conflict recovery.

Financial fraud during wartime is multifaceted, ranging from procurement fraud to digital scams. Fraudulent procurement is particularly prevalent, as emergency contracting procedures bypass traditional checks and balances. Perpetrators

[1] This chapter was prepared as part of a research project 0123U101945

establish shell companies to bid for lucrative contracts, delivering substandard or non-existent goods. For example, investigations into conflict zones have revealed instances where contractors supplied defective military gear or falsified documents for medical supplies.

Table 1.1 – Examples of wartime financial fraud schemes

Type of Fraud	**Mechanism**	**Example**	**Impact**
Procurement Fraud	False bidding, shell companies	Defective military supplies	Loss of critical resources
Cyber Fraud	Phishing, system infiltration	Hacking aid organizations	Diversion of humanitarian funds
Charity Fraud	Fake fundraising campaigns	Misappropriation of public donations	Erosion of donor trust and reduced aid effectiveness
Document Forgery	Manipulation of official records	False claims for compensations	Inefficient allocation of aid

Another significant type is cyber fraud, which includes phishing campaigns targeting relief organizations. In one case, hackers successfully infiltrated the financial systems of a major aid organization, redirecting millions in funds meant for displaced persons. Charity fraud also thrives, with fake fundraising campaigns diverting public contributions to personal accounts instead of humanitarian efforts.

Money laundering evolves in conflict settings to obscure the origins of illicit funds (Tab.1.2). The integration of laundered

funds into legitimate financial channels, such as reconstruction projects, poses a critical challenge. Cryptocurrencies, with their decentralized nature, are increasingly exploited for laundering activities, facilitating anonymous cross-border transactions.

Trade-based laundering remains another common method, where manipulated invoices are used to move money covertly. In Syria, for example, funds from illicit drug trade were funneled through manipulated agricultural export documents. This illustrates how economic sectors in conflict zones become conduits for financial crimes.

Table 1.2 – Money laundering channels in conflict zones

Method	Description	Example
Cryptocurrency Transactions	Anonymity and lack of regulation	Use of Bitcoin for arms funding
Trade-Based Laundering	Manipulated invoices to conceal funds	Over-invoicing agricultural exports
Real Estate Investments	Purchase of distressed properties	Hidden profits through undervalued properties

Corruption in wartime undermines governance, creating systemic inefficiencies (Tab.1.3). High-level embezzlement of aid funds often goes unchecked due to weakened institutional frameworks. For example, during the war in Afghanistan, significant portions of international aid were misappropriated through inflated defense contracts.

Bribery also becomes widespread in resource allocation, where access to food, shelter, and medical supplies is contingent upon payments to officials. Such practices deepen inequalities and exacerbate the suffering of vulnerable populations. Additionally, corruption within military budgets leads to inefficiencies in conflict management and undermines defense capabilities.

Table 1.3 – Wartime corruption practices and consequences

Practice	Description	Consequence
Embezzlement of Aid Funds	Diversion of humanitarian aid	Reduced impact of aid programs
Bribery for Resource Access	Payments required for essential supplies	Increased inequality among affected populations
Defense Budget Manipulation	Inflated contracts for personal gain	Weakening of national defense capabilities

The shadow economy thrives during wartime due to the collapse of formal markets and increased regulatory controls (Tab.1.4). Smuggling networks emerge to supply essential goods like fuel and medicine. For example, in Libya, smuggling operations have provided a significant revenue stream for militias, perpetuating conflict and instability.

Counterfeit currency production also increases, destabilizing local economies. In some conflict zones,

counterfeit money circulates alongside legitimate currency, undermining economic stability and trust in financial systems.

Table 1.4 – Shadow economy activities in wartime

Activity	**Description**	**Example**
Smuggling	Illicit trade of goods and services	Fuel smuggling in Libya
Informal Labor Markets	Exploitation of displaced populations	Low-wage work without legal protections
Counterfeit Currency	Production and distribution of fake money	Circulation in weakened economies

Organized crime networks adapt rapidly to wartime conditions, leveraging both traditional methods and modern technology. Arms trafficking, for instance, flourishes in regions with weak border controls. Simultaneously, human trafficking networks exploit displaced populations, with victims subjected to forced labor or sexual exploitation.

Digital transformation has enhanced the efficiency of these networks. Dark web platforms facilitate the exchange of illicit goods, while encrypted communications enable real-time coordination. Cryptocurrency transactions further complicate enforcement by providing anonymous financial flows.

The unchecked proliferation of financial crimes in wartime has far-reaching consequences.

Table 1.5 – Modern adaptations of organized financial crime

Activity	**Traditional Methods**	**Digital Enhancements**
Arms Trafficking	Physical smuggling routes	Online marketplaces for weapon sales
Human Trafficking	Direct exploitation networks	Recruitment through social media platforms
Illicit Financial Transfers	Cash-based money laundering	Anonymized cryptocurrency transactions

Economically, it diverts resources crucial for humanitarian relief and reconstruction. Socially, it exacerbates inequalities and undermines trust in institutions. Politically, it destabilizes governance structures, prolonging conflict and hindering recovery efforts.

To counter these crimes effectively, a multi-pronged approach is necessary:

1. Strengthening governance – enhanced oversight of aid flows and reconstruction funds through transparent mechanisms.

2. Leveraging technology – utilizing blockchain, artificial intelligence, and data analytics for monitoring and prevention.

3. International collaboration – fostering cross-border partnerships for intelligence sharing and coordinated enforcement.

4. Capacity building –training financial intelligence units and law enforcement to address evolving threats.

Understanding and addressing wartime financial crimes is not only crucial for immediate conflict management but also for ensuring sustainable peace and development in post-conflict regions. Future research should focus on the interplay between emerging technologies and financial crimes, as well as the development of predictive models to preempt these activities.

In conclusion, the schemes of financial fraud, money laundering, corruption, shadow economy, and organized crime during wartime are intricately connected to the socio-economic vulnerabilities of conflict-affected regions. By identifying and addressing these schemes, policymakers and practitioners can mitigate their impacts and foster resilience in affected communities.

1.2. Financial fraud, money laundering, corruption, shadow economy, and organized financial crime in wartime: insights from countries engaged in military conflict[2]

Military conflicts have consistently created environments where financial crimes thrive, exploiting the vacuum left by weakened governance and disrupted institutional frameworks. The intersection of armed conflict and financial crime is marked

[2] This chapter was prepared as part of a research project 0123U101945

by a notable increase in financial fraud, money laundering, corruption, the proliferation of shadow economies, and the activities of organized crime networks. These phenomena leverage the instability of conflict zones, leading to significant economic and social repercussions. The vulnerabilities of conflict-affected regions to financial crimes stem from the diversion of state resources to war efforts, the erosion of regulatory oversight, and the emergence of informal economic structures. In such conditions, illicit activities not only proliferate locally but often integrate into global financial systems, presenting a dual challenge of local destabilization and international economic risks.

The global interconnectedness of financial systems amplifies the impact of wartime financial crimes, allowing illicit funds to permeate legitimate markets. Transactions involving conflict-driven revenues often bypass conventional oversight mechanisms, utilizing methods such as informal value transfer systems, offshore accounts, or cryptocurrencies. These challenges necessitate a deeper understanding of how military conflicts exacerbate financial vulnerabilities and create opportunities for economic exploitation. Addressing this gap, this chapter seeks to analyze the interplay between financial crimes and armed conflicts, emphasizing the global implications and the need for coordinated responses.

Examining conflicts since 1990, the scope of this analysis extends across regions deeply affected by war. In Africa, nations like the Democratic Republic of Congo (DRC), Angola, and Sudan have experienced conflicts fueled by the exploitation of natural resources, such as diamonds, oil, and minerals. In the Middle East, countries including Iraq, Syria, and Yemen illustrate how smuggling, corruption, and informal trade networks become entrenched during prolonged instability. Eastern Europe provides a contemporary lens, with the Russia-Ukraine conflict showcasing the disruption of financial systems and the rise of organized crime exploiting wartime conditions. Meanwhile, in Asia, Afghanistan and Sri Lanka underscore the role of narcotics trafficking and informal financial systems in sustaining conflicts. These diverse cases highlight the multifaceted nature of financial crimes in wartime, offering insights into the economic mechanisms that both drive and are driven by armed conflicts.

The historical context of financial crime during wartime is best understood through the lens of global military conflicts since 1990. This period has witnessed a variety of wars, ranging from civil conflicts to large-scale international interventions. These wars have not only devastated economies but also dismantled governance structures, creating conditions conducive to illicit financial activities. For instance, the rise of

civil wars, as seen in Liberia, Sierra Leone, and Burundi, demonstrates how internal strife creates economic chaos, often with transnational implications. Conflicts in countries like Syria and the DRC have spilled over into neighboring regions, exacerbating their economic and financial challenges. Resource-driven wars, particularly in Angola and South Sudan, underscore how valuable commodities such as oil and diamonds become focal points for both conflict and associated financial crimes.

Table 1.6 provides an overview of conflicts, highlighting their periods, key characteristics, and economic impacts. This table emphasizes how specific conflicts have fostered financial crimes by undermining formal economic and governance structures.

A detailed examination of conflicts, their characteristics, and economic impacts reveals patterns that are critical for understanding the dynamics of wartime financial crimes. Afghanistan's prolonged conflict, fueled by narcotics trade, highlights how illicit financial flows become entrenched over decades. Algeria's civil war showcases how state resources are diverted during prolonged insurgencies. Bosnia and Herzegovina's ethnic war illustrates the embezzlement of international aid, a recurring issue in conflict zones.

Table 1.6 – Overview of conflicts and their characteristics

Country	Conflict Period	Key Characteristics	Economic Impact
Afghanistan	1992–2021	Prolonged insurgencies, narcotics trade	Significant illicit financial flows
Algeria	1991–2002	Civil war, insurgent activities	Diversion of state resources
Bosnia and Herzegovina	1992–1995	Ethnic conflict, international intervention	Embezzlement of international aid
Democratic Republic of Congo	1996–2003, ongoing	Resource-driven wars	Exploitation of natural resources
Iraq	1990–2003, ongoing	Gulf War, insurgencies	Misappropriation of oil revenues
Ukraine	2014–present	Annexation of Crimea, large-scale invasion	Corruption in military procurement
Syria	2011–present	Civil war, regional spillovers	Illicit trade and narcotics trafficking

The DRC's resource-driven wars provide a stark example of how natural resource exploitation feeds both local and international criminal networks. Iraq's Gulf War and subsequent insurgencies demonstrate the misappropriation of oil revenues, while Ukraine's ongoing conflict underscores the role of corruption in military procurement. Syria's civil war, with its regional spillovers, highlights the integration of illicit trade and narcotics trafficking into conflict economies.

Table 1.7 outlines the predominant financial crimes during wartime, linking them to specific mechanisms, affected countries, and their broader impacts on conflict dynamics.

Table 1.7 – Key financial crimes in wartime

Type of Financial Crime	Common Mechanisms	Example Countries	Impact on Conflict Dynamics
Financial Fraud	Smuggling, overpricing in military contracts	Afghanistan, Iraq	Prolongs conflicts through resource diversion
Money Laundering	Use of informal financial systems	Syria, DRC	Funds insurgencies and organized crime
Corruption	Misuse of humanitarian aid, ghost contracts	Bosnia, Ukraine	Undermines post-conflict reconstruction
Shadow Economy	Black-market trade in goods and arms	Somalia, Syria	Erodes formal economic structures
Organized Crime	Resource exploitation, narcotics trafficking	DRC, Afghanistan	Fuels transnational criminal networks

As highlighted in Table 1.7, financial crimes such as money laundering and corruption erode the capacity of states to recover from conflict, while shadow economies and organized crime perpetuate instability. This broad analysis sets the stage for a deeper exploration of mechanisms through which financial crimes exploit wartime conditions, emphasizing the need for targeted interventions. The interplay between local vulnerabilities and global financial systems underscores the

critical importance of addressing wartime financial crimes not only for immediate conflict resolution but also for long-term economic stability and security.

Financial fraud during wartime is a pervasive phenomenon that exploits the instability and chaos of conflict-affected regions. It manifests through several mechanisms, each capitalizing on the vulnerabilities of disrupted economies and weakened governance. A notable mechanism is illicit trade financing, wherein smuggling and black-market transactions are utilized to fund both state and non-state actors. These operations often involve essential goods, military supplies, or contraband, creating a shadow network of financial exchanges that bypass formal oversight.

Fraudulent procurement in military operations is another significant avenue of financial fraud. Wartime spending, particularly on defense and logistics, provides ample opportunities for inflated contracts, kickbacks, and ghost suppliers. This form of fraud not only drains public resources but also undermines the effectiveness of military operations, prolonging conflicts and deepening societal costs.

Smuggling operations, closely tied to illicit trade financing, thrive in wartime conditions. These activities range from the movement of arms and narcotics to the trafficking of precious resources like gold and diamonds. Smuggling networks

often operate across porous borders, leveraging the absence of coordinated enforcement mechanisms to maximize profits. These networks are frequently linked to organized crime groups, amplifying their scope and impact.

The examples of financial fraud during wartime provide insight into the diverse manifestations of this phenomenon. In Afghanistan, corruption in international aid management has been a persistent issue, with significant amounts of foreign assistance misappropriated or siphoned into private accounts. Iraq, during and after the Gulf War, witnessed the diversion of oil revenues through schemes like the "Oil-for-Food" program, which became a global scandal. Ukraine's ongoing conflict has highlighted misappropriation in reconstruction funds, where resources intended for rebuilding infrastructure are redirected for personal gain or used to sustain fraudulent networks. In Sudan, the exploitation of humanitarian aid during civil wars has been rampant, with large portions of aid being diverted to fund local militias. In Angola, illicit oil sales during the prolonged civil war became a major source of income for both government forces and rebel groups. Similarly, in the Democratic Republic of Congo, profits from illegal mining of coltan and diamonds were laundered through neighboring countries, financing prolonged violence and organized crime networks.

Table 1.8 – Examples of financial fraud in wartime

Country	Type of Fraud	Description
Afghanistan	Corruption in aid management	Misappropriation of foreign assistance funds
Iraq	Diversion of oil revenues	Misuse of funds under the "Oil-for-Food" program
Ukraine	Misappropriation of reconstruction funds	Redirection of resources for personal gain
Sudan	Diversion of humanitarian aid	Funding local militias during civil wars
Angola	Illicit oil sales	Financing government and rebel forces
DRC	Illegal mining profits	Laundering through neighboring countries

This analysis demonstrates the critical need for robust anti-fraud mechanisms tailored to wartime conditions. Addressing the systemic vulnerabilities that enable such crimes is essential not only for mitigating immediate economic damage but also for ensuring long-term recovery and stability in post-conflict regions. The interplay between illicit financial activities and armed conflicts underscores the importance of international collaboration, advanced monitoring systems, and adaptive policy frameworks to combat financial fraud effectively.

Money laundering in conflict zones represents a profound threat to financial stability and governance, particularly in areas already destabilized by warfare. The exploitation of conflict-driven resources and the breakdown of formal regulatory systems create fertile ground for the proliferation of illicit financial flows. Informal financial systems, such as hawala

networks and underground banking operations, are integral to laundering processes during wartime. These systems provide a covert mechanism for transferring funds, bypassing conventional oversight mechanisms, and ensuring anonymity for both recipients and facilitators. Offshore accounts further exacerbate this issue, serving as secure repositories for illicit revenues derived from resource exploitation, smuggling operations, and other criminal enterprises.

In Syria, the enduring civil war has led to the development of extensive cross-border smuggling networks. These networks are intricately tied to laundering operations, transforming illicit revenues from drug trafficking into legitimate assets integrated within regional economies. The Democratic Republic of Congo (DRC) offers another compelling example, where the illegal extraction and sale of mineral resources such as coltan and diamonds have fueled laundering activities, often facilitated by intermediaries in neighboring countries. Libya illustrates the nexus of resource exploitation and laundering, with oil revenues systematically diverted through smuggling routes and processed via international financial conduits, including Malta-based networks.

Table 1.9 – Detailed examples of money laundering in conflict zones

Country	Laundering Mechanism	Specific Examples	Impact
Syria	Cross-border laundering	Drug trafficking profits moved through Turkey	Strengthened insurgent groups
DRC	Exploitation of mineral resources	Coltan sold via Rwanda, laundered funds reinvested	Funded armed militias
Libya	Smuggling routes	Oil revenues laundered through Malta-based networks	Sustained local conflicts

As shown in Table 1.9, the mechanisms and examples of money laundering during wartime highlight the adaptability of illicit networks. The capacity of these operations to exploit weak governance and leverage transnational systems underscores the challenges faced by regulators and policymakers in conflict and post-conflict scenarios. The enduring impacts of these activities include prolonged conflicts, weakened state institutions, and reduced capacity for economic recovery.

Corruption during wartime is similarly amplified by the urgency and opacity that characterize conflict-driven governance. Military spending, expedited without rigorous oversight, becomes a prime target for corrupt practices. Inflated procurement contracts, ghost soldiers listed on payrolls, and the misallocation of funds drain essential resources. Humanitarian

aid, intended as a lifeline for affected populations, is often diverted for personal enrichment or political leverage. Political manipulation of financial systems during conflicts further entrenches systemic corruption, enabling elites to consolidate economic control under the guise of emergency governance.

Afghanistan exemplifies these trends through widespread corruption in military spending, with practices such as ghost soldiers on payrolls undermining the operational effectiveness of its armed forces. Ukraine's reconstruction efforts amid its ongoing conflict have exposed systemic corruption in infrastructure projects, including mismanagement in road construction and public utilities. In Sudan, the diversion of international humanitarian aid to support political elites and militias illustrates the misuse of resources intended for conflict mitigation.

As highlighted in Table 1.10, the corruption patterns in these conflict zones illustrate the multifaceted challenges of addressing governance failures during and after conflicts. These examples reinforce the necessity for comprehensive anti-corruption strategies, bolstered by international cooperation and mechanisms for accountability. Policymakers must address the root causes of corruption while fostering transparency and trust in post-conflict governance structures to ensure sustainable recovery and stability.

Table 1.10 – Comparative trends in wartime corruption

Country	Corruption Area	Specific Examples	Impact
Afghanistan	Military spending	Ghost soldiers drawing salaries, inflated arms contracts	Reduced military efficiency
Ukraine	Infrastructure rebuilding	Misuse of funds in road construction projects	Delayed post-conflict recovery
Sudan	Humanitarian aid	Diversion of food aid to militias	Increased civilian suffering, prolonged conflict

The shadow economy in wartime is an inevitable consequence of institutional collapse and societal disruption. The breakdown of formal institutions removes regulatory oversight, enabling the proliferation of unregulated economic activities. Economic survival strategies, where individuals and communities seek informal means of trade and sustenance, further fuel the shadow economy. Black-market operations become particularly dominant, serving as alternative systems for the exchange of goods and services, often at the expense of legal markets.

Key sectors impacted by the shadow economy during conflicts include the arms trade, illicit drugs, and counterfeit goods. These sectors thrive on the absence of regulation and the high demand for contraband. In Somalia, for example, the black-market arms trade has flourished amidst decades of civil war,

providing weapons to militias and non-state actors while undermining state authority. Iraq's shadow economy has historically served as a financial backbone for insurgencies, where smuggling and illicit trade in oil, antiques, and drugs generate substantial revenue. In Sri Lanka, the protracted civil conflict led to the development of extensive informal trade networks, enabling the transport of essential goods across conflict lines while evading governmental control.

As highlighted in Table 1.11, the drivers and examples of shadow economies underscore their adaptability and persistence in conflict zones. These activities not only sustain conflict dynamics but also create entrenched systems that challenge post-conflict economic recovery.

Table 1.11 – Key drivers and examples of shadow economies in wartime

Driver	Examples	Impact
Breakdown of formal institutions	Somalia: arms trade	Strengthened militias, erosion of state control
Economic survival strategies	Sri Lanka: informal trade networks	Sustained civilian livelihoods, evasion of taxes
Black-market operations	Iraq: smuggling of oil and artifacts	Funding of insurgencies, loss of state revenue

Organized financial crime networks adapt remarkably to wartime conditions, leveraging instability to expand their operations. Cybercrime, for instance, has become increasingly

prevalent, with hackers targeting financial institutions and aid organizations to divert funds. Cross-border trafficking, encompassing drugs, arms, and human trafficking, is another hallmark of these networks. Resource monopolization, particularly in regions rich in natural resources, allows organized crime groups to consolidate control over valuable commodities, often funding armed conflicts.

Regional case studies provide vivid illustrations of these phenomena. In West Africa, diamond smuggling in Sierra Leone has been instrumental in financing prolonged conflicts, with illicit trade routes stretching across multiple countries. In the Middle East, the production and trafficking of Captagon – a potent amphetamine – have surged during Syria's civil war, generating billions in revenue for organized crime groups and militias. Eastern Europe presents the example of arms trafficking in Ukraine, where weapons have been smuggled through porous borders, fueling both local and international black markets.

As detailed in Table 1.12, the adaptation of organized crime networks to wartime conditions demonstrates their capacity to exploit geopolitical instability. These activities not only finance conflicts but also establish transnational networks that persist beyond the cessation of hostilities. Addressing the challenges posed by organized financial crime requires

coordinated international efforts, robust regulatory frameworks, and targeted interventions tailored to the unique conditions of each conflict zone.

Table 1.12 – Organized financial crime networks in wartime

Region	Activity	Examples	Impact
West Africa	Diamond smuggling	Sierra Leone: conflict diamonds	Funded prolonged conflicts
Middle East	Drug production	Syria: captagon trafficking	Sustained militias, destabilized region
Eastern Europe	Arms trafficking	Ukraine: smuggling across borders	Fueled black markets, strengthened insurgencies

Policy and countermeasures aimed at mitigating financial crimes in wartime require a comprehensive and multifaceted approach. The implementation of international frameworks plays a pivotal role in addressing cross-border financial crimes. Anti-Money Laundering (AML) measures form the backbone of these efforts, encompassing the monitoring of suspicious transactions, enhancing financial institution compliance, and fostering international cooperation through platforms such as the Financial Action Task Force (FATF). These measures aim to disrupt the movement of illicit funds and prevent their integration into formal financial systems.

Technological solutions, including blockchain technology, offer innovative tools to enhance transparency and

traceability in financial transactions. Blockchain's immutable ledger capabilities ensure that illicit activities are more easily detectable, reducing the potential for fraud and money laundering. Additionally, digital forensics tools can be deployed to track and analyze cybercrime activities, which are often intertwined with organized financial crimes during conflicts.

Strengthening local governance and transparency is equally critical. Building the capacity of local regulatory bodies to enforce financial regulations, improve oversight mechanisms, and foster accountability is essential. Transparency initiatives, such as public financial disclosure systems and independent audits, help reduce opportunities for corruption and mismanagement.

Post-conflict reconstruction strategies must prioritize economic reforms and institutional capacity-building to restore stability and resilience. Economic reforms should focus on revitalizing formal financial markets, addressing the structural causes of shadow economies, and reintegrating conflict-affected regions into global trade networks. Simultaneously, building institutional capacity involves training personnel, modernizing regulatory frameworks, and fostering partnerships between public and private sectors to rebuild trust in financial institutions.

Table 1.13 – Policy and countermeasures for combating financial crimes in wartime

Category	Specific Measures	Expected Impact
Anti-Money Laundering	Monitoring suspicious transactions, FATF compliance	Disruption of illicit fund flows
Technological Solutions	Blockchain, digital forensics	Enhanced transparency and traceability
Governance and Transparency	Public financial disclosures, independent audits	Reduced corruption and increased accountability
Economic Reforms	Revitalizing financial markets, trade reintegration	Stabilization of local economies
Institutional Capacity-Building	Training, regulatory modernization	Strengthened resilience of financial institutions

The policies outlined in Table 1.13 emphasize a multi-dimensional approach to combat financial crimes in wartime. Anti-Money Laundering (AML) measures focus on disrupting illicit fund flows through rigorous monitoring and compliance standards like FATF guidelines. Technological innovations, including blockchain, enhance transaction transparency, making it harder for illicit activities to go unnoticed. Governance and transparency measures ensure accountability in public finances, while targeted economic reforms aim to revitalize economies affected by conflict. Building institutional capacity ensures long-term resilience and prepares financial systems to handle future challenges effectively. Together, these strategies form a

cohesive framework for addressing financial crimes during and after conflicts.

1.3 Financial fraud, money laundering, corruption, shadow economy and organized financial crime in wartime: a dynamic analysis of scientific publications[3]

The study of financial fraud, money laundering, corruption, shadow economies, and organized financial crime in wartime reveals critical insights into the dynamics of conflict-affected economies and their broader implications. These phenomena are not isolated disruptions but systemic issues that exploit the vulnerabilities of states during crises, perpetuating instability and undermining recovery efforts. The academic investigation of these topics is essential for understanding the interplay between financial crimes and societal breakdowns during wars, enabling the formulation of more effective counterstrategies.

Financial crimes in wartime are deeply intertwined with the erosion of state institutions and the emergence of alternative power structures. Corruption flourishes in environments where oversight is weak, and shadow economies expand as citizens

[3] This chapter was prepared as part of a research project 0123U101945

resort to informal means of survival. Organized financial crime networks adapt rapidly to exploit the chaos, leveraging illicit resource monopolization, cross-border trafficking, and cybercrime. These dynamics not only deepen economic disparities but also challenge global security by sustaining conflict economies.

The global academic response to these issues has generated a rich body of research spanning multiple disciplines, including economics, political science, law, and international relations. This body of work offers diverse perspectives on the causes, mechanisms, and consequences of financial crimes in wartime, but it also reflects significant fragmentation in terms of thematic focus and methodological approaches.

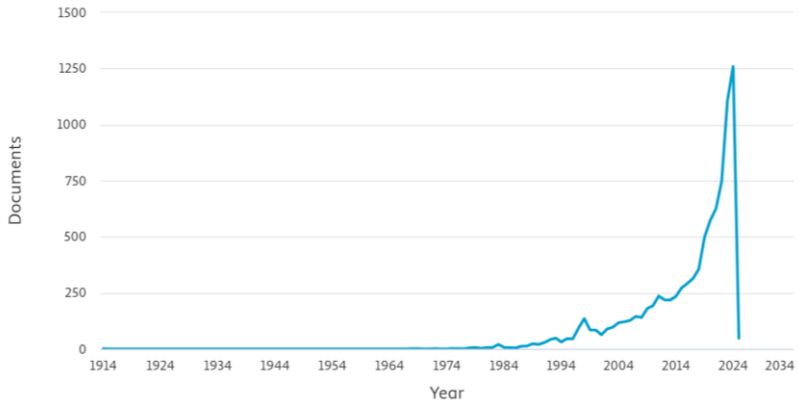

Figure 1.1 – Global dynamics of scientific publications on financial fraud (1914–2024)

The trend in academic publications addressing "financial fraud" as indicated by Scopus demonstrates a substantial and continuous growth over recent decades. From the early 20th century until the 1980s, there was minimal academic output on this topic. The graph shows that only a few scattered publications were recorded annually, reflecting limited global attention to financial fraud in academia during this period.

Starting in the 1990s, a noticeable uptick in publications began, coinciding with the increased globalization of financial markets and the associated rise in complex financial crimes. This period also witnessed significant advancements in information technology, which both enabled new forms of fraud and facilitated more comprehensive studies of financial crimes.

The 2000s marked a steep increase in publication volume, likely influenced by major financial scandals (e.g., Enron, WorldCom) and the subsequent regulatory changes like the Sarbanes-Oxley Act in the U.S. The global financial crisis of 2008 further accelerated academic interest, as scholars sought to understand the systemic weaknesses that allowed fraud to proliferate in global markets. This spike is reflected in the graph, showing consistent annual growth in publications post-2008.

The most dramatic growth occurred in the 2010s and early 2020s, with the annual number of publications rising

exponentially. This growth aligns with several key developments:

1. The rapid digitization of financial systems, leading to the emergence of cyber fraud as a critical area of study.

2. Increasing global regulatory focus on anti-money laundering (AML) and combating the financing of terrorism (CFT).

3. A growing recognition of the interconnectedness between financial fraud, corruption, and other organized crimes.

The peak observed in 2024, with over 1,200 publications, underscores the heightened academic interest in financial fraud and related issues during recent years. This surge may also reflect the aftermath of global crises, such as the COVID-19 pandemic and geopolitical conflicts, which intensified financial vulnerabilities worldwide.

1. Exponential growth (the volume of research on financial fraud has shown exponential growth, particularly in the last decade).

2. Research drivers (key drivers include global financial crises, regulatory reforms, and the increasing sophistication of financial crimes).

3. Recent peaks (the record high in 2024 suggests an unprecedented level of academic engagement, possibly fueled

by contemporary challenges such as cryptocurrency fraud and wartime financial crimes).

This dynamic underscores the urgent need for continued research into financial fraud, particularly in contexts like wartime and emerging technologies, where vulnerabilities are most pronounced.

Building upon the general dynamics of publication trends, the distribution of research outputs across specific academic sources reveals critical insights into the thematic and institutional focus of studies on financial fraud and related topics. Figure 1.2 shows the contribution of various journals and conference proceedings to the discourse, highlighting their role in shaping the academic landscape.

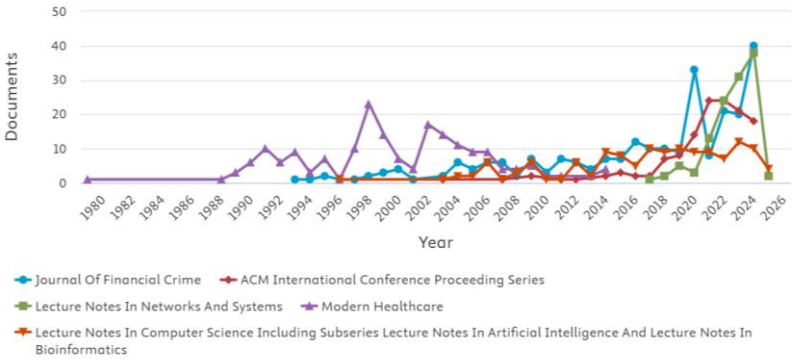

Figure 1.2 – Distribution of publications on financial fraud across leading journals and conferences (1980–2024)

The Journal of Financial Crime leads with 246 publications, cementing its position as a cornerstone for research dedicated to financial fraud, money laundering, and corruption. Its sustained prominence reflects the journal's specialization in addressing both theoretical frameworks and practical countermeasures to financial crimes. This is followed by Modern Healthcare with 188 articles, indicating an interdisciplinary approach where the financial management aspects of healthcare systems intersect with fraud detection and prevention.

Other notable contributors include:

– Lecture Notes in Computer Science, which published 134 documents. This aligns with the growing incorporation of artificial intelligence and machine learning techniques in fraud detection and prevention systems;

– ACM International Conference Proceedings Series and Lecture Notes in Networks and Systems, collectively emphasizing the technological and systemic dimensions of financial fraud;

– Specialized journals like the Journal of Business Ethics and IEEE Access, with their respective focuses on ethical considerations and technological advancements, further diversify the academic output;

The temporal analysis of these sources highlights fluctuations in publication volumes over the years. Peaks correspond to global crises, such as the 2008 financial crash and the COVID-19 pandemic, underscoring the reactive nature of academic research to systemic shocks. For instance:

– a surge in the Lecture Notes in Computer Science during recent years aligns with the increasing application of computational tools in analyzing financial crimes.

– the Journal of Financial Crime exhibits consistent growth, reflecting its role as a primary repository of specialized knowledge.

These findings emphasize the interdisciplinary nature of research in this field, with contributions spanning ethics, technology, and applied financial systems. As the volume of publications continues to grow, these sources play a pivotal role in disseminating knowledge, fostering collaboration, and guiding practical implementations in combating financial crimes.

The Figure 1.3 highlights the distribution of scientific publications on "financial fraud" across various countries and territories, providing insights into the geographic concentration of research efforts.

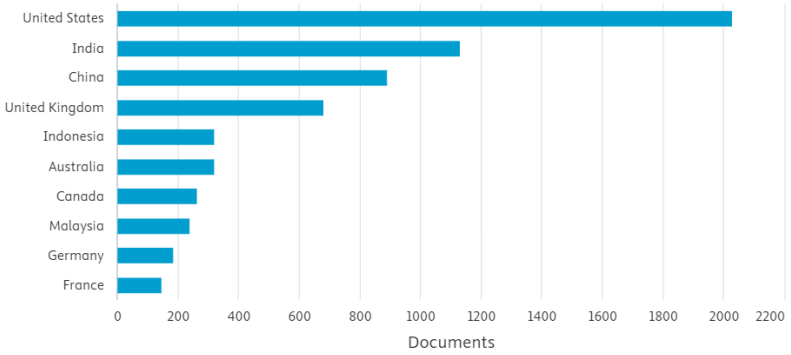

Figure 1.3 – Geographic distribution of publications on financial fraud by country (Scopus Data, 1914–2024)

Key observations:

1. The United States dominates the field with 2,026 publications, reflecting its robust academic infrastructure, extensive financial markets, and a history of addressing financial crimes through research and policy development. Factors contributing to this dominance include the country's proactive approach to combating financial fraud and the presence of leading institutions and funding agencies that prioritize research in this area.

2. India ranks second with 1,129 publications, followed by China with 889. This indicates the growing academic interest in financial fraud in these rapidly developing economies. In India, the rise in research output may be linked to increased instances of financial scams and the implementation of digital

financial systems. China's focus could be attributed to its expanding financial sector and the challenges associated with regulating complex financial transactions.

3. With 678 publications, the United Kingdom demonstrates a strong tradition of research into financial fraud, likely supported by its advanced regulatory systems and international financial hubs like London.

4. Indonesia and Australia follow closely, contributing 319 and 318 publications, respectively. These figures underscore the relevance of financial fraud as a research focus in diverse economic and regulatory contexts.

5. Canada (260 publications) and European countries such as Germany (184 publications) and France (not shown but likely significant) contribute notably, reflecting their commitment to understanding and addressing financial fraud on both domestic and international levels.

6. With 237 publications, Malaysia's growing contribution reflects its strategic position in Southeast Asia and its active engagement in research addressing financial crimes within the context of emerging markets.

The geographic distribution of research indicates that financial fraud is a global issue, with significant contributions from both developed and developing economies. The concentration of research in countries like the United States and

India demonstrates the interplay between the prevalence of financial crimes, the size of financial markets, and the prioritization of this topic in academic and policy circles. At the same time, contributions from regions like Southeast Asia highlight the increasingly globalized nature of financial systems and the need for international collaboration in combating fraud.

The distribution of academic contributions to research on financial fraud, categorized by institutional affiliation (Fig. 1.4), provides valuable insights into the institutions driving knowledge production in this critical field. The data presented highlights the leading universities and research institutions that have significantly advanced the study of financial crimes.

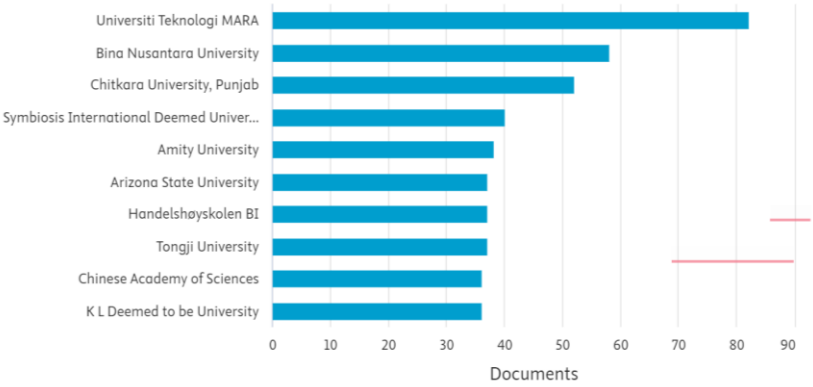

Figure 1.4 – Leading academic institutions in financial fraud research (Scopus Data, 1914–2024)

At the forefront of this academic effort is Universiti Teknologi MARA, which leads with 82 publications. This institution's dominance reflects its targeted focus on financial fraud research, particularly in the context of Southeast Asia. This achievement is likely the result of dedicated research initiatives and regional collaborations addressing financial crimes.

Other significant contributors from Southeast Asia include Bina Nusantara University (58 publications) and Chitkara University, Punjab (52 publications). These institutions underline the growing engagement of the region's academic community in tackling financial fraud through both theoretical and applied research.

Institutions from other parts of the world also demonstrate strong involvement. Arizona State University **(**37 publications) in the United States and Handelshoyskolen BI (37 publications) in Europe showcase their contributions to the global understanding of financial fraud. The presence of Tongji University and the Chinese Academy of Sciences highlights China's growing commitment to integrating advanced technological solutions into financial crime research.

The contributions from Symbiosis International Deemed University (40 publications) and Amity University (38 publications) in India reflect the country's expanding interest in this field, particularly in the context of a rapidly digitizing

economy. These institutions signify the broad spectrum of research approaches and regional contexts that define financial fraud scholarship globally.

Figure 1.5 highlights the leading authors in the field of financial fraud research, as identified through Scopus data. It showcases the individual contributions that have significantly shaped the academic landscape in this domain.

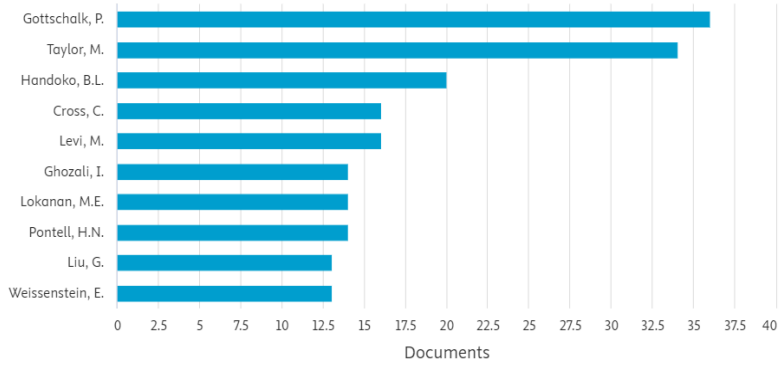

Figure 1.5 – Top authors contributing to research on financial fraud (Scopus Data, 1914–2024)

Leading contributors:

1. Gottschalk, P. – leads the field with 36 publications. His prolific contributions likely reflect a focus on criminology, organizational fraud, and white-collar crime.

2. Taylor, M. – follows closely with 34 publications, indicating significant engagement in topics related to fraud detection, risk management, and financial governance.

Active researchers:

1. Handoko B.L. has 20 publications, emphasizing the growing importance of interdisciplinary approaches, particularly in regions addressing emerging financial fraud challenges.

2. Cross C. and Levi M. both contribute 16 publications each, demonstrating their strong influence in financial crime and legal frameworks.

Regional and Methodological Diversity:

1. Researchers such as Pontell, H.N. and Weissenstein, E. have contributed foundational studies, likely focusing on the intersections of sociology, economics, and law enforcement strategies.

2. Ghozali, I. and Lokanan, M.E. have added value through regionally focused studies, highlighting the unique characteristics of financial fraud in specific economic or cultural contexts.

The diverse range of authors emphasizes the interdisciplinary and international nature of financial fraud research. This diversity highlights the importance of addressing both global and localized challenges in combating financial crimes.

The prominence of these authors underscores the critical role of individual researchers in advancing the understanding of financial fraud. Their contributions have not only provided

theoretical insights but also practical frameworks for tackling complex financial crimes. Future research can build on their work to address evolving threats in an increasingly digitalized financial ecosystem.

Figure 1.6 provides a breakdown of the types of documents contributing to the body of research on financial fraud. It illustrates the various formats through which academic insights are disseminated, offering a comprehensive view of how knowledge in this domain is shared.

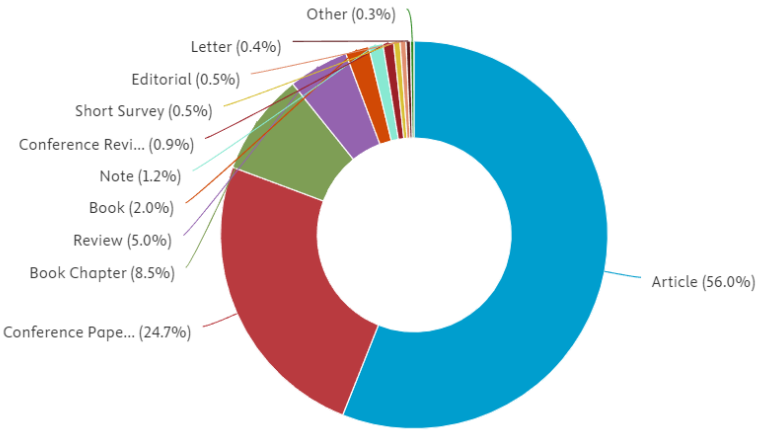

Figure 1.6 – Distribution of publications on financial fraud by document type (Scopus Data, 1914–2024)

Figure 1.6 shows that the majority of publications (56%, 5,068 documents) are journal articles. This highlights the preference for peer-reviewed articles as the primary medium for

disseminating research findings on financial fraud, ensuring rigorous academic standards and widespread accessibility.

Conference papers account for 24.7% (2,231 documents) of the total. This reflects the dynamic and fast-paced nature of research discussions in this field, often driven by advancements in technology and emerging trends in financial crimes.

Book chapters (8.5%, 772 documents) and reviews (5%, 456 documents) play a critical role in consolidating knowledge, providing theoretical frameworks, and offering synthesized insights into existing research.

Books represent 2% (177 documents) of the total, indicating the development of comprehensive works addressing financial fraud. Additionally, notes (1.2%, 108 documents), conference reviews (0.9%, 81 documents), and short surveys (0.5%, 49 documents) demonstrate the diversity of contributions, often focusing on niche topics or emerging issues.

Editorials (0.5%, 44 documents) and letters (0.4%, 36 documents) provide platforms for thought leadership, opinions, and concise discussions on timely issues in financial fraud research.

Given the critical intersection of financial fraud, corruption, and wartime conditions, future investigations should focus on analyzing the dynamics of scientific publications across these domains. Specifically, exploring temporal trends and

thematic shifts in publications using keywords such as "financial fraud," "corruption," and "military conflicts" can reveal patterns of academic focus and gaps in existing literature. Such an approach would not only enrich the understanding of how these phenomena evolve during crises but also help identify underexplored areas requiring attention.

To address these research gaps, will explore the dynamics of scientific publications, examining the relationships between financial fraud, corruption, and military conflicts. This investigation will focus on the evolution of thematic priorities, the density of academic collaborations, and emerging trends that shape the global research agenda in this field.

A targeted analysis of scientific publications using specific keyword combinations reveals the following results:

– the combination "financial fraud" AND "military conflicts" yielded 3 documents in total. This limited number suggests a highly specialized and underexplored intersection of financial fraud and military conflicts.

– searching for "financial fraud" AND "war" resulted in 50 documents**,** indicating moderate academic interest. These studies likely explore the implications of financial crimes in the broader context of wartime economies and reconstruction efforts.

– the combination "corruption" AND "war" produced a significantly larger body of research, with 1,842 documents identified. This result highlights corruption as a dominant theme in studies addressing wartime governance, resource allocation, and economic disruptions.

– similarly, "corruption" AND "military conflict" yielded 248 documents**,** underscoring a focused yet substantial academic interest in corruption's role within military and conflict scenarios.

In order to ensure that the analysis remains comprehensive and structured, priority research areas have been identified with a balance between breadth and specificity. Given the volume of publications, the following areas are the most suitable for further study:

1. "Corruption" AND "military conflict" – **t**his thematic combination offers a sufficient number of studies to enable a detailed analysis while maintaining a clear focus on the interactions between corruption and conflict dynamics.

2. "Financial AND fraud" and "war" – while this dataset is smaller, it presents a unique opportunity to delve into the nuanced challenges of financial fraud in wartime economies, providing insights into regulatory failures and illicit financial flows during crises.

By concentrating on these thematic areas, the subsequent analysis can explore the evolving trends, methodologies, and geographic distributions of research, shedding light on critical intersections of financial crimes, governance, and wartime conditions. Figure 1.7 represents the yearly distribution of 50 documents retrieved from Scopus based on the keywords "financial AND fraud" and "war" over the period 1969–2024. The data highlights a relatively sparse academic focus on this intersection, with notable fluctuations in research outputs.

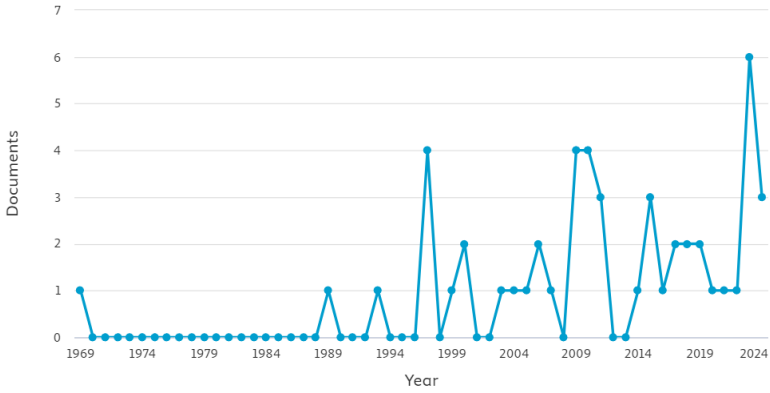

Figure 1.7 – Temporal distribution of publications on «Financial Fraud» and «War» (Scopus Data, 1969–2024)

Key trends:

– early period (1969–1993) – minimal publications, reflecting limited academic exploration of financial fraud in wartime contexts during these decades.

– growth phase (1994–2014) – periodic spikes in publication numbers, likely corresponding to global events, including conflicts where financial fraud gained prominence in policy and academic discussions.

– recent activity (2015–2024) – a notable increase in publications, particularly in 2023 (6 documents) and 2024 (3 documents), demonstrating a growing academic interest in the implications of financial fraud within wartime economies.

Figure 1.8 illustrates the temporal evolution of 248 documents based on the keywords "corruption" and "military AND conflict" from 1984 to 2024. It reveals a consistent upward trajectory in publications, indicating a sustained and expanding academic interest in this critical intersection.

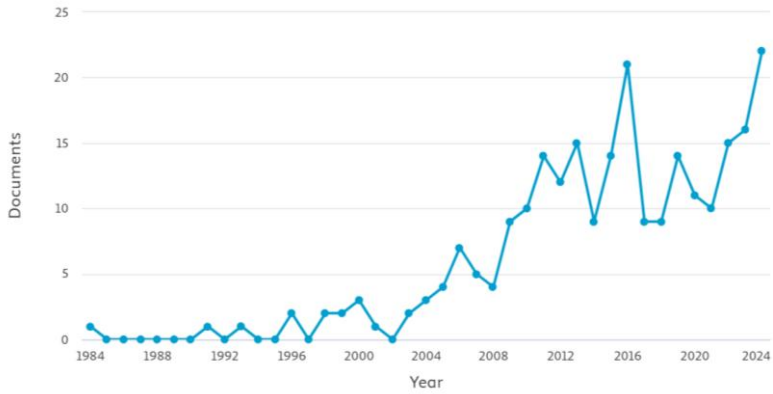

Figure 1.8 – Trends in publications on corruption and military conflicts (Scopus Data, 1984–2024)

Key trends:

– initial period (1984–2000) – sparse and incremental growth in publications, reflecting early academic engagement with the topic;

– expansion phase (2001–2016) – steady increases, marked by periodic peaks likely driven by high-profile conflicts and related corruption challenges;

– recent surge (2017–2024) – a sharp increase in publications, peaking at 22 documents in 2024. This underscores the growing recognition of corruption's critical role in exacerbating and sustaining military conflicts.

These two figures collectively highlight the different levels of academic engagement with "financial fraud and war" versus "corruption and military conflicts." While research on financial fraud in wartime remains relatively niche, the significant growth in studies on corruption and military conflicts reflects broader acknowledgment of governance challenges in conflict zones. Both themes warrant further exploration to address the multifaceted impacts of financial crimes and corruption on global security and post-conflict recovery.

Figure 1.9 highlights the distribution of 50 documents by country or territory based on the Scopus search for the keywords "financial AND fraud" and "war." The data emphasizes the

geographic concentration of academic research efforts on this thematic intersection.

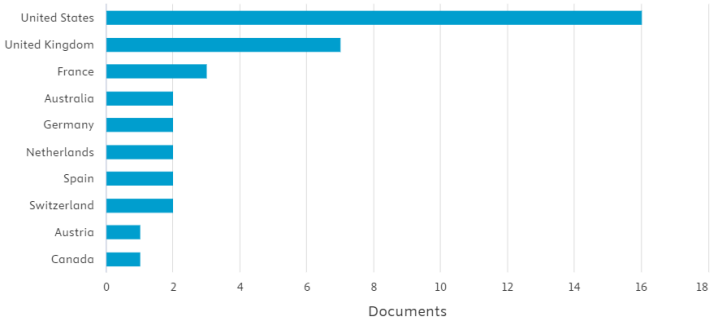

Figure 1.9 – Geographic distribution of publications on financial fraud and war (Scopus Data, 1969–2024)

Figure 1.9 shows that:

– with 16 publications, the United States demonstrates a dominant role in this area, reflecting its advanced academic infrastructure and focus on financial crimes in global contexts.

– ranking second with 7 publications, the United Kingdom underscores its strong academic tradition in researching wartime financial fraud.

– France (3 publications) and Germany (2 publications) highlight moderate contributions from Europe, while countries like the Netherlands and Switzerland also participate in this discourse.

– Australia (2 publications) and Canada (1 publication) showcase the involvement of countries outside Europe and North America in advancing this field.

Figure 1.10 displays the geographic distribution of 248 documents from Scopus, retrieved using the keywords "corruption" and "military AND conflict." The data showcases a broader engagement with this topic compared to financial fraud and war, indicating a more global academic focus.

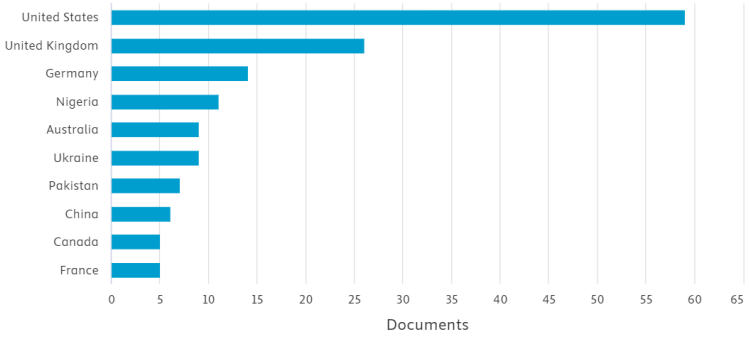

Figure 1.10 – Geographic Distribution of Publications on Corruption and Military Conflicts (Scopus Data, 1984–2024)

Key insights from Figure 1.10:

– leading with 59 publications, the United States again demonstrates a strong commitment to researching corruption's role in military conflicts;

– with 26 publications, the United Kingdom plays a significant role in advancing research in this area;

– countries like Germany (14 publications), Nigeria (11 publications), and Ukraine (9 publications) highlight the engagement of both developed and developing nations.

– contributions from Australia (9 publications), Pakistan (7 publications), and China (6 publications) emphasize the global scope of research on corruption and military conflicts.

These figures illustrate the varying levels of global academic engagement with the two topics. While the United States leads in both areas, the broader range of contributing countries in research on corruption and military conflicts reflects the global urgency of addressing governance issues in conflict zones. In contrast, financial fraud in wartime remains a more specialized and less geographically dispersed research focus. This disparity highlights the need for increased international collaboration to bridge these thematic and regional gaps in the academic discourse.

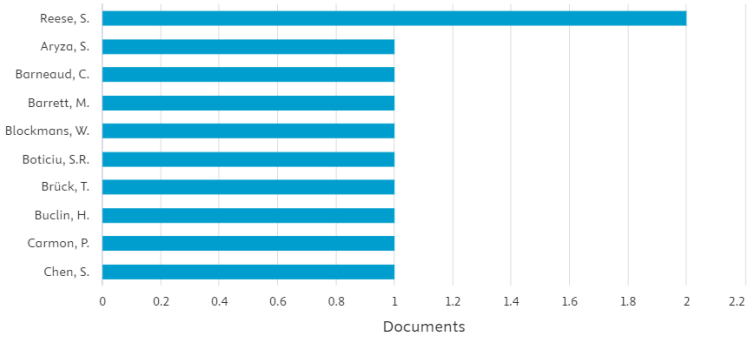

Figure 1.11 – Top Authors on Financial Fraud and War (Scopus Data, 1969–2024)

Figure 1.11 presents the distribution of publications by authors focusing on the intersection of "financial fraud" and "war" based on Scopus data. The dataset highlights 50 documents authored by various contributors, with limited concentration of works per individual. Key observations:

– Reese S., leads with 2 publications, indicating modest contributions to this niche field;

– most authors, including Aryza S., Barneaud C., and Blockmans, W., have authored only one publication, reflecting a dispersed and specialized research focus;

– the distribution suggests that research in this domain remains scattered, with opportunities for more cohesive academic exploration.

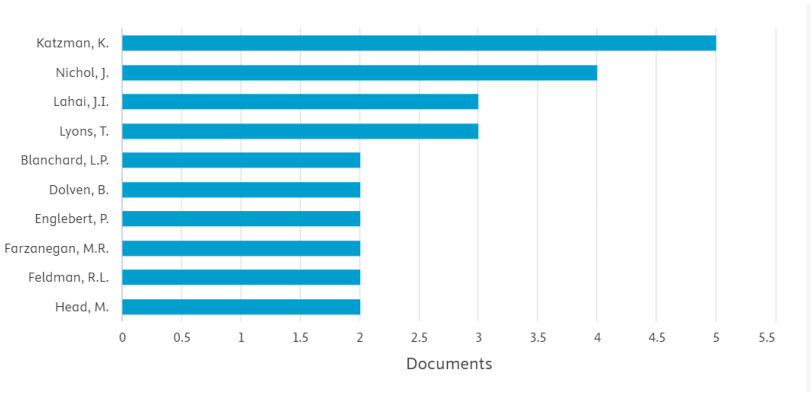

Figure 1.12 – Top Authors on Corruption and Military Conflicts (Scopus Data, 1984–2024)

Figure 1.12 shows the distribution of publications by authors contributing to the intersection of "corruption" and "military AND conflict" based on Scopus data. The dataset includes 248 documents, reflecting a broader engagement with this research area. Key observations:

– Katzman K., leads with 5 publications, followed by Nichol, J., with 4. These authors have significantly shaped the discourse in this area.

– Authors such as Lahai J.I., and Lyons T., each with 3 publications, reflect a growing academic focus on corruption within military conflict contexts.

– The presence of multiple contributors with 2 publications each, such as Blanchard L.P., and

Farzanegan M.R., underscores the potential for collaborative studies to consolidate research efforts.

The two figures highlight distinct trends in the contributions of individual authors to the respective themes. Research on "financial fraud and war" appears to be an emerging and underexplored area with low author concentration. In contrast, "corruption and military conflicts" shows a more robust and diverse authorial base, suggesting higher academic interest and a more established research community. These insights point to the need for increased academic collaboration and focused studies to advance the understanding of financial fraud and corruption in wartime settings.

The analysis of scientific publications based on keywords such as "financial fraud", "corruption", "war", and "military conflict", using Scopus data, highlights the critical importance of conducting dynamic analysis to explore these complex and interconnected phenomena. The graphs and tables reflecting temporal trends, geographical distribution, leading author contributions, and document types reveal the following key aspects:

1. The significant growth in publications on corruption and military conflicts, particularly over the last decade, underscores the increasing attention to these issues at both academic and policy levels. This demonstrates the need for an

in-depth analysis of shifts in research priorities to better understand global challenges associated with financial crimes during wartime.

2. The distribution of publications by country and institution shows substantial geographic diversity. Countries such as the United States, the United Kingdom, Germany, and emerging economies like Ukraine and Nigeria are actively shaping the academic discourse. Understanding how geopolitical and economic contexts influence research in this area is vital for a comprehensive perspective.

3. The publication trends over time highlight the cyclical nature of academic interest, driven by specific military conflicts and their consequences. Peaks in publication numbers often coincide with globally significant events, such as the Iraq War, the Syrian conflict, or the full-scale invasion of Ukraine.

4. The analysis of leading authors in corruption and military conflict research reveals the presence of influential scholars who form the foundation for further scientific advancements. At the same time, the relatively isolated nature of publications on financial fraud in wartime indicates the need to foster greater collaboration among researchers to broaden knowledge in this niche area.

5. The prevalence of journal articles, conference papers, and book chapters demonstrates the multidisciplinary nature of

this topic, offering opportunities for diverse approaches to its study.

Dynamic analysis serves as a critical tool for future research, as it enables:

– identification of patterns in academic interest regarding financial crimes and corruption in military conflicts;

– recognition of knowledge gaps and priority areas for further exploration;

– promotion of global collaboration and the development of practical recommendations to address financial crimes in wartime contexts;

– by leveraging dynamic analysis, researchers can not only expand the theoretical understanding of these issues but also contribute to the effective implementation of scientific findings into policy and economic strategies aimed at mitigating financial crimes during and after military conflicts.

1.4. Financial fraud, money laundering, corruption, shadow economy and the organised financial crime in wartime: the clustering of academic achievements by the branching or concentration of research networks[4]

The study of financial fraud, money laundering, corruption, shadow economies, and organized financial crime in the context of wartime necessitates a thorough understanding of the global academic landscape. As research on these topics spans multiple disciplines, regions, and institutions, clustering analysis emerges as a pivotal methodological approach to unravel the structure, dynamics, and interconnectedness of academic achievements. Clustering analysis enables the identification of patterns, relationships, and trends within large datasets, making it an invaluable tool for examining the concentration or branching of research networks. By grouping related publications, researchers, and institutions based on thematic and methodological similarities, clustering analysis provides insights into the most active research hubs, key contributors, and collaborative networks driving scientific progress in this domain. Such an approach is particularly relevant for topics as complex and interdisciplinary as financial crimes in wartime,

4 This chapter was prepared as part of a research project 0123U101945

where knowledge production is dispersed across diverse academic fields such as economics, political science, law, and criminology. In the context of wartime financial crimes, clustering academic achievements offers several benefits. First, it allows for the identification of dominant research themes and their evolution over time, shedding light on the shifting priorities of the academic community. Second, it reveals the geographic and institutional concentration of research efforts, highlighting the regions and organizations that lead global discourse. Third, clustering analysis facilitates the exploration of cross-disciplinary collaborations, uncovering the intersections between fields such as cybersecurity, international law, and conflict studies, which are critical for addressing the multifaceted nature of financial crimes. Moreover, the ability to visualize and interpret academic clusters enhances the strategic planning of future research. By identifying gaps in existing literature and underrepresented regions or topics, clustering analysis supports the development of targeted initiatives that bridge these gaps. Additionally, understanding the density and strength of connections within research networks helps foster international collaboration and knowledge sharing, both of which are essential for addressing global challenges such as financial fraud and corruption in wartime settings. This section aims to apply clustering analysis to explore the academic

achievements in the field of wartime financial crimes. By examining the geographic and institutional affiliations of researchers, identifying research leaders, and mapping the density of connections between academic schools, this analysis seeks to uncover the underlying structure of the research landscape. The insights gained will not only contribute to a deeper understanding of existing achievements but also inform the strategic direction of future studies and international partnerships in this critical area of research.

The clustering of academic achievements related to financial fraud, money laundering, corruption, shadow economy, and organized financial crime in wartime was conducted using bibliometric analysis tools, specifically VOSviewer. The analysis involved the following stages:

1. Relevant publications were identified from the Scopus and WoS databases using keywords such as "financial fraud", "corruption", "shadow economy" and "war." Co-occurrence of terms in titles, abstracts, and keywords was used as the basis for analysis.

2. Using the bibliometric software, a co-occurrence network was generated, where nodes represented key terms, and edges indicated the strength of their co-occurrence. The resulting visualization presented clusters of related concepts based on thematic proximity.

3. The network was divided into distinct clusters using modularity optimization. Each cluster was assigned a unique color to distinguish thematic areas.

4. Each cluster was analyzed to identify its central themes, key terms, and research focus areas. This interpretation provided insights into the dominant topics and interdisciplinary connections within each cluster.

The contextual clustering of research is shown in Figure 1.13.

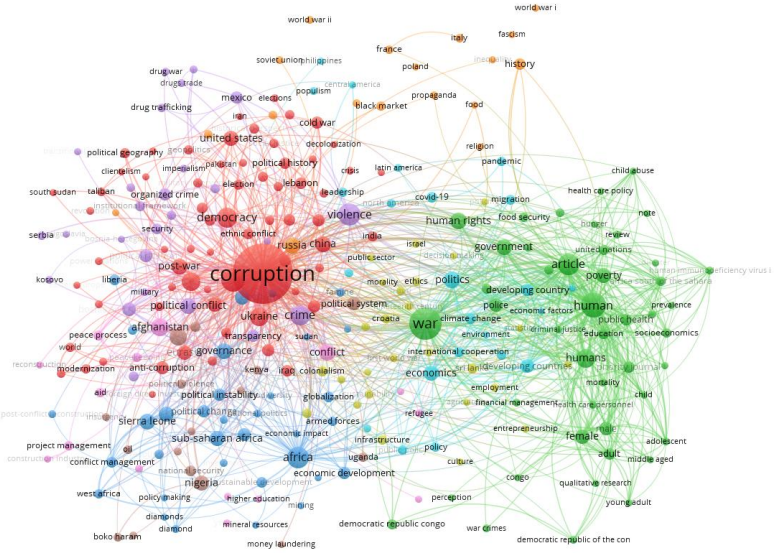

Figure 1.13 – Contextual clustering of academic research on "financial fraud", "corruption", and "organized financial crime" in wartime contexts

Cluster 1 (Red). This cluster is centered around terms such as "corruption," "political conflict," "governance," "violence," "democracy," and "organized crime." Research in this cluster explores the intersection of corruption and political instability during wartime. Studies highlight the role of governance in mitigating corruption, the influence of organized crime in exacerbating conflict, and the broader implications for democracy and societal stability. Additionally, this cluster includes discussions on post-conflict reconstruction and the role of international aid in addressing systemic corruption.

Cluster 2 (Green). The green cluster focuses on "war," "economics," "human rights," "employment," "public health," and "social welfare." This cluster captures research on the socio-economic impacts of war, including displacement, unemployment, and public health crises. Studies investigate how financial fraud and corruption undermine humanitarian efforts, highlighting the importance of transparency and accountability in post-conflict recovery.

Cluster 3 (Blue). Central themes in this cluster include "document forgery," "financial management," "public relations," "legal aspects," "business ethics," and "standards." Research in this area examines the mechanisms of financial and document fraud, the role of public relations in exposing fraudulent activities, and the ethical and legal frameworks

necessary to prevent such crimes. The interplay between governance and financial management is also a key focus.

Cluster 4 (Yellow). This cluster revolves around "history," "international cooperation," "World War II," "humanitarian aid," and "global governance." Studies explore historical instances of financial crimes during wartime, drawing lessons from past conflicts to address contemporary challenges. The cluster emphasizes the role of international cooperation in combating transnational financial crimes.

Cluster 5 (Purple). Key terms in this cluster include "drug trafficking", "black market", "money laundering", and "criminal networks." Research focuses on the role of organized crime in exploiting wartime economies through illicit trade and money laundering. Studies highlight the need for robust international frameworks to combat cross-border financial crimes.

Cluster 6 (Orange). This cluster is characterized by terms like "policy-making," "anti-corruption," "transparency," and "institutional development." Research explores the effectiveness of public policies and anti-corruption strategies in mitigating the economic impacts of war. Emphasis is placed on institutional reforms and the development of global anti-corruption standards.

The rest of the clusters contain only a few keywords each, so they are not considered in the context of contextual clustering.

The clustering analysis reveals the multifaceted nature of financial crimes during wartime. Each cluster represents a unique aspect of this complex phenomenon, ranging from corruption and organized crime to socio-economic impacts and public policy responses. The diversity of topics underscores the importance of interdisciplinary research and collaboration in addressing the challenges posed by financial crimes in conflict settings. Future research can build on these findings by exploring cross-cluster linkages and developing integrated strategies to combat financial crimes effectively.

Figure 1.14 represents the density map of academic publications related to the themes of corruption, war, governance, and associated socio-political and economic factors. This density visualization is generated based on the co-occurrence of keywords extracted from academic articles indexed in Scopus. The map illustrates the frequency and strength of connections between concepts, allowing us to identify core topics and peripheral trends within the research domain.

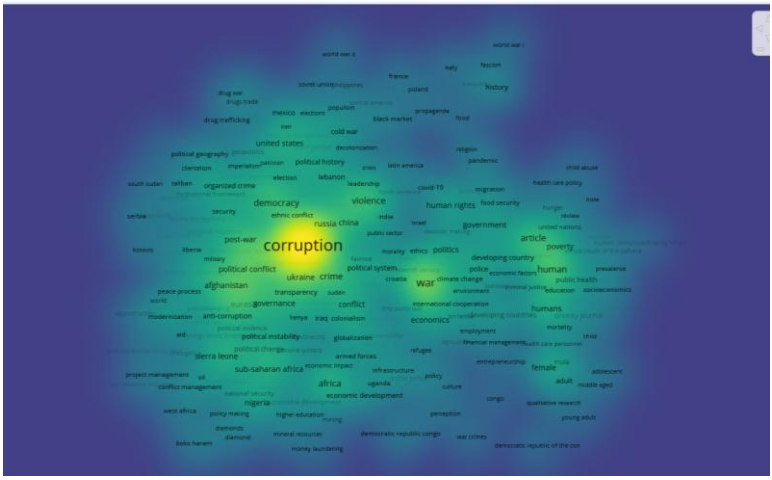

Figure 1.14 – Density visualization of academic research on "financial fraud", "corruption", and "organized financial crime" in wartime contexts

According to Figure 1.14 main characteristics are:

1. The term "corruption" occupies a central and densely populated position, indicating its pivotal role in the academic discourse. It is closely linked to topics such as "governance," "political conflict," "transparency," "democracy," and "violence." This suggests that much of the research focuses on the relationship between corruption and political instability, especially in conflict-prone regions.

2. "War" is another significant node, linked to terms like "human," "government," "economics," "poverty," and "human

rights." This highlights the intersection of military conflicts with socio-economic and humanitarian concerns.

– Peripheral but notable themes include "Financial fraud", "money laundering " "organized crime," "drug trafficking," "black markets," and "aid," reflecting the broader economic and criminal dynamics associated with corruption and war.

3. Specific regional references such as "Ukraine," "Russia," "China," "Africa," "Afghanistan," and "Sierra Leone" indicate that research often centers on these geopolitically significant areas.

4. Terms like "ethics," "public health", "poverty," and "education" suggest an interdisciplinary approach, integrating social, economic, and health perspectives.

Insights from the figure 1.14:

– the high-density regions around "corruption" and "war" reflect the prevalence of these issues in academic discussions. Their connections to diverse themes, such as governance, economic development, and human rights, highlight the multifaceted nature of the research;

– the inclusion of terms like "pandemic" and "COVID-19" shows the adaptability of the research focus to contemporary global challenges;

– the map underscores the integration of political science, economics, sociology, and public health in addressing issues related to corruption and conflict.

This density visualization serves as a powerful tool for understanding the thematic priorities and interconnections in academic research, providing a foundation for targeted exploration of under-researched areas and promoting cross-disciplinary collaboration. Temporal contextual clustering (figure 1.15) offers a comprehensive view of how the academic discourse on financial fraud, corruption, money laundering, shadow economies, and organized financial crime evolves over time.

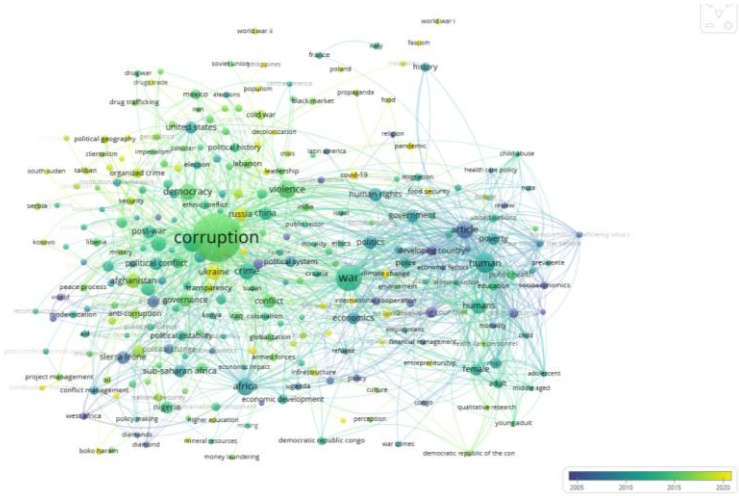

Figure 1.15 – Temporal-contextual visualization of academic research on "financial fraud", "corruption", and "organized financial crime" in wartime contexts

By integrating temporal data with thematic clusters, this analysis allows researchers to identify trends, emerging themes, and the dynamics of academic focus in the context of wartime and post-war periods. Such an approach is invaluable for:

1. Identifying shifts in academic priorities and the emergence of new subfields over specific timeframes.

2. Highlighting how academic output aligns with or anticipates real-world challenges, such as the rise in financial crimes during wartime or post-conflict reconstruction phases.

3. Revealing interconnected research topics across disciplines and regions, fostering collaboration and interdisciplinary innovation.

4. Providing insights into future areas of interest by understanding current trajectories and knowledge gaps.

Table 1.14 shows the structured result of temporal contextual clustering based on visualization.

By mapping the progression of academic focus, this clustering not only delineates how global challenges have shaped research priorities but also provides a roadmap for addressing future issues in the field. Researchers and policymakers can utilize these insights to bridge academic knowledge and practical solutions effectively.

Table 1.14 – Results of Temporal Contextual Clustering

Cluster	Time Period (Dominance)	Central Themes	Key Concepts
Cluster 1	2005–2010	Corruption and Governance	Political instability, governance, democracy, international cooperation
Cluster 2	2010–2015	Financial Fraud and Policy	Anti-corruption, governance, financial regulations, public policy
Cluster 3	2015–2020	War and Economic Impact	Armed conflicts, economic resilience, post-war recovery, refugee crises
Cluster 4	2008–2020	Public Health and Development	Health policy, public sector management, humanitarian aid, socio-economic factors
Cluster 5	2000–2010	Organized Crime Networks	Drug trafficking, human trafficking, cross-border smuggling, security threats
Cluster 6	2010–2020	Shadow Economies	Informal trade, illicit resource extraction, black markets, regional dynamics
Cluster 7	2005–2020	Cybercrime and Digital Economies	Cyber fraud, digital currencies, technological solutions, blockchain
Cluster 8	2008–2020	Conflict Regions and Global Politics	Middle East, sub-Saharan Africa, post-colonial transitions, power dynamics
Cluster 9	2010–2020	Legal and Ethical Standards	Business ethics, legal frameworks, compliance, international regulations

Analyzing the data in the table, the following key clusters should be noted:

– Cluster 1 (corruption and governance) — predominantly active during 2005–2010, this cluster reflects early academic interest in understanding the role of governance and political stability in mitigating corruption, especially in post-conflict nations.

– Cluster 2 (financial fraud and policy) – between 2010 and 2015, attention shifted toward the development and enforcement of policies aimed at tackling financial fraud, signaling a growing recognition of its systemic risks.

– Cluster 3 (war and economic impact) – this cluster highlights the interconnectedness of war and economic stability, focusing on recovery mechanisms and the financial challenges faced by conflict-affected regions.

– Cluster 7 (cybercrime and digital economies) – emerging as a dominant theme in the last decade, this cluster underscores the increasing relevance of cybercrime and technological advancements in financial crimes.

Next figure – 1.16 illustrates the network visualization of collaboration among countries in research related to financial fraud, corruption, and economies in wartime conditions. The visualization is based on a bibliometric analysis of collaborative efforts between authors from various countries, represented as nodes (circles). The connections between nodes indicate co-authorship or interaction within scientific networks.

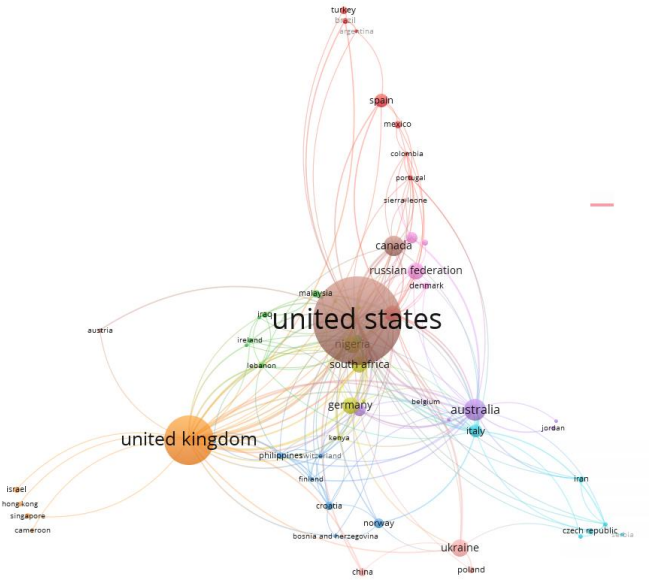

Figure 1.16 – Network visualization of international collaboration in research on financial fraud, corruption, and wartime economies

Figure 1.16 shows that the largest node corresponds to the United States, highlighting its dominant position in research on this topic. The U.S. exhibits strong collaborative links with many other countries, including those in Europe (e.g., the United Kingdom, Germany) and Asia (e.g., Israel, China).

The United Kingdom also plays a significant role in the network, with notable connections to European, Asian, and African countries. This reflects its multifaceted approach to international scientific collaboration.

Smaller nodes, such as Ukraine, Nigeria, and Australia, show active participation in regional research. Ukraine, in particular, demonstrates collaborations with European countries, reflecting its focus on studying the impacts of war on financial systems.

Clusters of collaboration:

– North American cluster with the United States at its core.

– European Cluster featuring strong interactions between the United Kingdom, Germany, and other EU countries.

– Asian-African cluster involving countries grappling with corruption and economic development challenges.

Some countries, such as those in the Middle East (e.g., Iran, Jordan), exhibit weaker connections to major nodes. This indicates the need for greater integration into global scientific networks.

This network underscores the diversity and interconnectedness of academic collaborations across regions while identifying areas for potential improvement in global research integration.

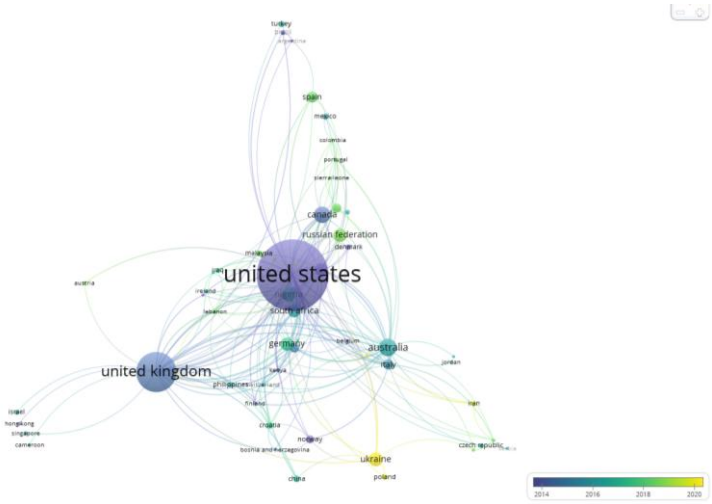

Figure 1.17 – Temporal overlay visualization of international collaboration in research on financial fraud, corruption, and wartime economies (2014–2020)

Figure 1.17 represents the temporal overlay of international collaboration networks in research related to financial fraud, corruption, and wartime economies. The size of each node corresponds to the number of publications, while the color gradient indicates the average publication year. Darker shades represent earlier years in the timeline, while brighter shades indicate more recent collaborations. The United States emerges as the most prominent hub, with extensive connections to the United Kingdom, Germany, and emerging regions such as South Africa and Ukraine.

The map highlights the evolution of research collaboration, demonstrating a notable increase in activity in the latter half of the observed period (2018–2020).

Table 1.15 summarizes the evolving trends in collaborative research on financial crimes, corruption, and governance in wartime, emphasizing the geographical and thematic expansion over time.

Table 1.15 – Characteristics by Year for the Temporal Overlay Visualization

Year Range	Key Characteristics	Key Countries	Themes and Focus
2014–2016	- Concentration in well-established hubs like the **United States** and **United Kingdom**. - Notable collaborations with **Germany** and **Russia** reflecting post-Soviet economic issues. - Initial focus on **South Africa**, signaling interest in transitional states.	United States, United Kingdom, Germany, Russia, South Africa	Governance, legal frameworks, policy mechanisms, transitional economies
2017–2018	- Expansion of research with **Australia**, **Nigeria**, and **Ukraine** emerging as key collaborators. - Ukraine gains importance due to its conflict and implications for corruption and shadow economies. - Regional dynamics of	United States, Australia, Nigeria, Ukraine	Corruption, governance in conflict zones, shadow economies, regional dynamics

	corruption in conflict zones emphasized.		
2019–2020	- Surge in research activity; **United States** remains a leader. - Stronger links with **Eastern Europe** (Ukraine) and **Africa**. - Emerging connections with **Turkey** and **China**, reflecting globalization of financial crimes and technological advancements.	United States, Ukraine, Nigeria, Turkey, China	Globalized financial crimes, cross-border money laundering, technological solutions

The donut (figure 1.18) chart represents the distribution of academic publications on topics related to corruption, financial fraud, and their intersections with armed conflicts and wars, categorized by subject areas from 2019 to 2023.

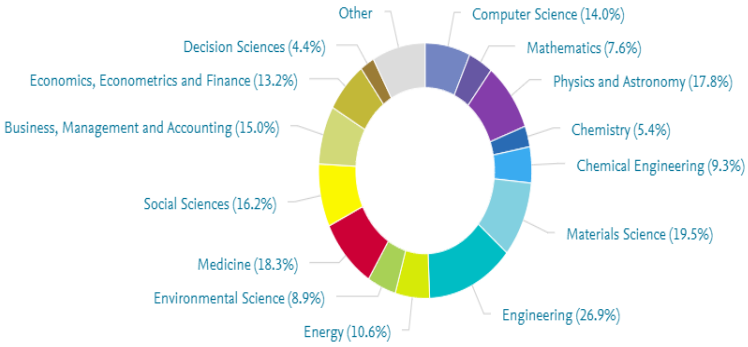

Figure 1.18 – Thematic distribution of publications on corruption and financial fraud during armed conflicts

Key insights include from figure 1.18:

– Engineering (26.9%) – emerges as the leading field, reflecting a significant focus on the technological aspects of combating corruption and fraud, such as cybersecurity and infrastructural resilience in conflict zones.

– Medicine (18.3%) – highlights research on the mismanagement of humanitarian aid and public health systems in war-affected regions, which are often prone to corruption.

– Materials Science (19.5%) – suggests exploration of illicit exploitation of natural resources and their impact on global supply chains during conflicts.

– Social Sciences (16.2%) – underscores the study of governance, political instability, and societal impacts of corruption during wartime.

– Business, Management, and Accounting (15.0%) – reflects a focus on financial systems, fraud detection, and economic recovery post-conflict.

– Economics, Econometrics, and Finance (13.2%) – addresses macroeconomic impacts, including illicit financial flows and the economic strategies of warring nations.

– Environmental Science (8.9%) – showcases research on environmental crimes linked to wars, such as illegal deforestation and pollution.

– Contributions in Physics and Astronomy (17.8%), Computer Science (14.0%), and Mathematics (7.6%) – emphasize the use of computational models, data analysis, and technological advancements in fraud detection and prevention.

This thematic distribution reflects the interdisciplinary nature of research in this domain, highlighting the critical importance of diverse academic approaches to understanding and mitigating corruption and financial fraud in the context of armed conflicts and wars.

The nexus of financial fraud, money laundering, corruption, and the shadow economy during wartime has gained significant scholarly attention. This review synthesizes academic literature globally, identifying key research directions, gaps, and implications for future investigations.

Key themes in the literature:

1. **Corruption and governance in wartime.** Numerous studies underscore how wartime conditions exacerbate corruption due to weakened governance and institutional collapse. Adebanwi and Obadare (2011) and Nwozor et al. (2020) critically assess Nigeria's anti-corruption efforts, highlighting political elite manipulation and selective prosecutions. Le Billon (2003) investigates the dual role of corruption in perpetuating conflict and facilitating fragile peace

agreements. Doig and Tisne (2009) further emphasize the challenges of reconstructing governance in post-war states.

In historical contexts, Wang (2017) explores corruption within the Guomindang government during World War II, illustrating the systemic issues that arose in resource allocation and bureaucratic inefficiency. Neudorfer and Theuerkauf (2014) analyze the role of corruption in increasing the likelihood of ethnic wars, emphasizing its destabilizing effects on already fragile societies.

2. **Money laundering and organized crime** Wartime environments often facilitate money laundering and organized crime. Bolodeoku (2009) discusses Nigeria's tax reforms to combat financial crime, while Jensen and Hapal (2018) analyze the interplay between police corruption and organized crime in the Philippines' war on drugs. Tromme and Otaola (2014) explore Mexico's anti-corruption commission and the political complexities of combating organized crime.

Garlepow et al. (2024) examine metaphorical representations of war and corruption in South Asian contexts, linking linguistic frames to organized financial crimes. These works highlight the transnational dynamics of financial crime, particularly in conflict zones.

3. **Shadow economy dynamics**. The shadow economy's growth during conflict is a recurrent theme in the

literature. Martin (2018) links informal markets to systemic corruption in African conflicts, while Chung (2024) focuses on socio-economic implications in South Korea's wartime economy. Uberti (2014) investigates the mining sector in post-war Kosovo, demonstrating how weak governance perpetuates shadow economic activities.

4. **Post-war transitions and corruption.** Post-war transitions often see corruption hindering recovery efforts. Lindberg and Orjuela (2014) and Lesschaeve and Glaurdić (2022) identify the legacies of war as significant obstacles to democratic accountability and institutional trust. Le Billon (2014) emphasizes the role of natural resource governance in post-war transitions, highlighting the importance of building trust to reduce corruption.

Miholic (2023) provides a historical perspective by examining medical corruption in post-World War I Vienna, demonstrating the enduring challenges of rebuilding societal trust after conflicts.

5. **Regional perspectives**. Regional studies offer valuable insights into the diverse manifestations of wartime corruption and financial crime. Orjuela et al. (2016) examine the ethnic divides in Sri Lanka's post-war corruption, while Maringira (2017) documents military corruption among Zimbabwean soldiers during their deployment in the Democratic

Republic of Congo. Cercel (2024) explores interwar Romania, revealing the historical roots of systemic corruption and its critique under fascist ideologies.

Ozden and Onapajo (2019) highlight Nigeria's use of anti-corruption policies in foreign relations under Buhari's administration, emphasizing their geopolitical implications.

6. **Technological and policy challenges**. The role of technology in financial crime has become increasingly significant. Nimko et al. (2024) examine e-governance's impact on corruption perception in Ukraine during wartime, identifying digital tools' dual role in mitigating and facilitating corruption. Fjelde (2009) investigates the role of oil wealth and resource management in fueling civil wars, linking economic policies to corruption dynamics.

Wedeman (2008) provides a longitudinal perspective on China's anti-corruption efforts, illustrating the interplay between political will, governance structures, and policy effectiveness.

Despite significant progress, several gaps remain:

– comparative analyses: limited studies compare wartime corruption across regions, leaving room for cross-cultural and institutional comparative research.

– transnational crime networks: the dynamics of transnational financial crime during conflicts remain underexplored, particularly in the digital age.

– longitudinal studies: few longitudinal studies examine how wartime corruption evolves into post-war economies, creating gaps in understanding long-term impacts.

– technological implications: the role of technology, including cryptocurrency in laundering wartime assets, requires further investigation.

The existing literature provides a solid foundation for understanding the interplay of financial fraud, corruption, and organized crime in wartime. However, addressing the identified gaps requires global, interdisciplinary, and technologically informed research efforts to mitigate these crimes' impact during and after conflicts.

Conclusions to chapter 1

The conducted analysis underscores the critical importance of studying financial fraud, money laundering, corruption, shadow economies, and organized financial crime in wartime contexts. These phenomena are not merely byproducts of instability but are deeply rooted systemic issues that exploit the vulnerabilities of conflict-affected regions, perpetuating economic disparities, weakening state institutions, and

exacerbating global security challenges. The study highlights that these crimes are interwoven with the breakdown of governance structures, the rise of shadow economies as survival mechanisms, and the proliferation of organized criminal networks.

By employing advanced bibliometric and network analysis techniques, this research has structured the global academic landscape, providing a comprehensive view of the thematic and temporal trends in scholarly contributions. The findings reveal several key insights into the evolution of research priorities, the geographic distribution of academic output, and the interdisciplinary nature of this field:

1. The research identifies distinct thematic clusters, including governance and anti-corruption, financial management and fraud detection, and the role of technology in combating financial crimes. Central themes such as corruption, organized crime, political instability, and public policy are deeply interconnected, reflecting the multidimensional nature of these challenges. Moreover, the integration of advanced technological solutions, such as blockchain and digital forensics, has emerged as a focal point in addressing financial crimes.

2. The analysis demonstrates significant contributions from both developed and developing nations. Countries like the United States and the United Kingdom are leaders in academic

output, driven by their robust research infrastructures and policy focus on financial crimes. Simultaneously, emerging economies such as Ukraine, Nigeria, and India are increasingly contributing to the discourse, reflecting their unique regional challenges and priorities. The interconnectedness between these countries highlights the globalized nature of financial crimes and the necessity for cross-border collaboration.

3. The clustering of academic achievements underscores the importance of institutional networks in shaping research trajectories. Leading universities and research hubs have played a pivotal role in advancing understanding and developing innovative approaches to mitigate financial crimes. Collaborative networks between institutions from diverse regions further emphasize the interdisciplinary and international nature of this research domain.

4. The temporal analysis reveals a significant increase in academic interest over the past two decades, with particular surges in publication activity during periods of heightened global conflict, such as post-2014. This trend underscores the evolving complexity of financial crimes in wartime and the need for adaptive and proactive research to address emerging challenges. The temporal clustering also highlights shifts in research priorities, from foundational studies on corruption and

governance to contemporary issues such as cybercrime and the use of advanced technologies in financial crime prevention.

5. The findings of this study have profound implications for policymakers and practitioners. The global and interconnected nature of these crimes necessitates comprehensive international frameworks that integrate governance, technology, and capacity-building. Targeted anti-money laundering measures, transparency initiatives, and post-conflict economic reforms must be prioritized to address the root causes of financial crimes. Furthermore, the integration of academic insights into policy development can significantly enhance the effectiveness of countermeasures.

6. The study highlights critical gaps in the existing literature, particularly in the understanding of regional dynamics, the interplay between corruption and organized crime, and the role of emerging technologies in financial crime prevention. Future research should focus on these underexplored areas, employing interdisciplinary approaches to develop holistic solutions. Comparative analyses of regional and national strategies can provide valuable insights into best practices and areas for improvement.

In conclusion, the study emphasizes that addressing financial fraud, money laundering, corruption, shadow economies, and organized financial crime in wartime requires a

coordinated and interdisciplinary effort. By leveraging academic insights, fostering international collaboration, and integrating technological innovations, the global community can develop robust strategies to combat these challenges effectively. This research not only contributes to the theoretical understanding of these phenomena but also provides actionable insights to guide policymakers, practitioners, and academics in their efforts to ensure economic and social resilience in conflict-affected regions.

CHAPTER 2. CYBERSECURITY AND THE COUNTERING OF ORGANISED AND TRANSNATIONAL CYBERCRIME IN WARTIME: AN OVERVIEW OF THE SCIENTIFIC LANDSCAPE AND INSIGHTS FROM COUNTRIES ENGAGED IN MILITARY CONFLICT

2.1. Foundations and challenges in cybersecurity and combating transnational cybercrime during wartime[5]

The digital era has revolutionized global interactions, economies, and governance systems, providing unparalleled opportunities for growth, innovation, and connectivity. However, it has also opened the door to new and highly sophisticated threats, among which cybercrime stands out as one of the most pervasive and challenging. When the stability of nations is further strained by war, the vulnerabilities in their digital ecosystems are amplified, presenting an unprecedented opportunity for organised and transnational cybercriminal networks. This intersection of warfare and cybercrime creates a multifaceted problem that demands urgent and detailed exploration.

The intersection of warfare and digital crime has transformed cybercrime into a strategic threat during military

5 This chapter was prepared as part of a research project 0124U000550

conflicts. Organised cybercrime during wartime is no longer a peripheral concern; it is a critical tool in hybrid warfare strategies. Nations engaged in military conflicts often experience significant disruptions to their digital infrastructure, with attacks targeting government systems, critical infrastructure, and even civilians. Cyberattacks in wartime extend far beyond economic loss – they are designed to destabilize societies, weaken institutions, and sow confusion in already fragile environments.

For instance, during the ongoing military conflicts in Ukraine, sophisticated cyberattacks have been documented, targeting governmental institutions, healthcare systems, and energy infrastructure. These attacks have crippled operational capacities and demonstrated the ability of cybercriminals to exploit wartime instability for both financial and geopolitical gains. Similar scenarios have been observed globally, from ransomware attacks on hospitals during armed conflicts in the Middle East to disinformation campaigns aimed at influencing public sentiment in Western democracies.

Organised cybercrime networks are uniquely positioned to exploit the vulnerabilities of nations at war. These networks operate across borders, leveraging the anonymity and vast reach of cyberspace to coordinate attacks with precision. Their schemes often involve the following elements:

– cybercriminals employ cutting-edge technologies, including artificial intelligence, blockchain, and deepfake software, to execute sophisticated attacks such as data breaches, phishing schemes, and ransomware.

– wartime conditions often lead to the diversion of resources away from cybersecurity, leaving critical systems such as healthcare, financial services, and public administration inadequately protected.

– in many cases, cybercrime networks align with state actors to conduct cyberwarfare, blurring the lines between crime and warfare. This collaboration adds another layer of complexity, as cybercriminals gain access to state resources and capabilities.

The transnational nature of these networks poses a unique challenge to law enforcement and policymakers. Unlike conventional warfare, cyberattacks do not recognize national boundaries, and perpetrators can operate from jurisdictions that lack robust cybersecurity laws or enforcement mechanisms. This complicates international cooperation and creates safe havens for cybercriminals.

In the context of modern warfare, research into cybersecurity and cybercrime is not merely an academic exercise; it is a strategic necessity. The global interconnectedness of cyberspace means that the consequences of cyberattacks during wartime extend far beyond the immediate

battlefield. They affect international markets, disrupt global supply chains, and challenge the international legal framework governing cyber operations.

The academic and practical investigation of organised and transnational cybercrime in wartime is essential for several reasons:

1. Research can identify the methodologies, tools, and targets of cybercriminals, providing a detailed understanding of how these networks operate during military conflicts.

2. Evidence-based insights are critical for developing effective policies and strategies to combat cybercrime. This includes not only national efforts but also international collaborations, given the transnational nature of the threat.

3. Research can drive the development of innovative technological solutions to counter cyber threats, such as advanced threat detection systems, encryption protocols, and cyber resilience frameworks.

4. In wartime, civilians are often the unintended victims of cyberattacks. Research can help design interventions that safeguard critical services such as healthcare and communication networks.

The study of cybercrime during wartime is not without its challenges. One of the primary issues is the lack of reliable data, as cyberattacks often go unreported or are misclassified.

Additionally, the rapidly evolving nature of cyber threats requires continuous adaptation of research methodologies and technologies. The geopolitical dimension further complicates the landscape, as the motivations and capabilities of cybercriminals are deeply intertwined with state interests.

Another critical challenge is the lack of consensus on international norms and regulations governing cyber operations in wartime. Despite efforts by organizations such as the United Nations, there is no universally accepted framework for defining and prosecuting cybercrimes committed during military conflicts. This regulatory gap leaves many nations vulnerable and highlights the urgent need for a coordinated global response.

Cybersecurity during wartime is not an isolated issue, it is part of a larger conversation about the role of technology in modern society and its implications for security, sovereignty, and human rights. Organised and transnational cybercrime during military conflicts serves as a stark reminder of the double-edged nature of technological progress. While technology can drive innovation and development, it can also be weaponized to exploit vulnerabilities and undermine societal stability.

In conclusion, the urgency of addressing organised and transnational cybercrime in wartime cannot be overstated. This chapter will provide a detailed exploration of the schemes

employed by cybercriminals during military conflicts and the measures that nations have taken to counter these threats. Through this analysis, it aims to contribute to the development of a comprehensive understanding of wartime cybersecurity and to propose actionable solutions for mitigating the risks posed by cybercrime.

2.2 Schemes of organized and transnational cybercrime in wartime[6]

Cybercrime during wartime is a highly specialized and dynamic phenomenon, fundamentally different from traditional cybercrime observed during peacetime. Military conflicts amplify the vulnerabilities of digital infrastructures, making them key targets for cyberattacks. These attacks are often strategically planned to disrupt societal stability, undermine governance, and destabilize economic systems. Understanding the unique characteristics of cybercrime in wartime is essential to developing effective countermeasures and resilience strategies.

6 This chapter was prepared as part of a research project 0124U000550

Military conflicts often bring about a complete restructuring of societal priorities, with a focus on physical survival, immediate defense, and resource mobilization. In this context, digital systems become both an asset and a liability. While digital networks facilitate communication, logistics, and international collaboration, they are also prone to exploitation by cybercriminals who take advantage of weakened oversight and chaotic conditions.

The integration of cybercrime into the broader spectrum of warfare – commonly referred to as hybrid warfare – has transformed it into a tool of strategic importance. Modern conflicts are no longer limited to physical battlefields but extend into cyberspace, where adversaries aim to cripple essential services, manipulate public opinion, and gain a tactical edge.

Characteristics that differentiate wartime cybercrime:

1. **Target selection and intent**. In wartime, cybercriminals often target critical national systems such as energy grids, water supplies, transportation networks, and healthcare facilities. Unlike peacetime attacks, which are usually motivated by financial gain, wartime cybercrime focuses on creating large-scale disruptions that: erode public trust in governance; delay or derail military operations.

During the 2015 Russian-Ukrainian conflict, cyberattacks targeted Ukraine's power grid, resulting in widespread blackouts

and showcasing the destructive potential of cyber operations on critical infrastructure.

2. **Collaboration between state and non-state actors.** The line between state-sponsored actors and independent cybercriminals becomes increasingly blurred during wartime. Criminal networks often collaborate with nation-states to achieve mutually beneficial objectives, such as espionage, disinformation, or resource theft.

In the Syrian Civil War, cybercriminals collaborated with state actors to infiltrate opposition networks, facilitating surveillance and control over dissenting groups.

3. **Exploitation of chaos and weakness**. Wars naturally weaken institutional oversight, as resources are diverted to immediate physical defense. Cybercriminals exploit this environment by targeting:

– financial systems (for fraud and money laundering);

– communication platforms (to spread disinformation or phishing campaigns);

– military logistics (to disrupt supply chains or intercept sensitive information).

In Yemen, ongoing conflict has led to widespread misuse of digital payment systems, allowing criminals to siphon international aid intended for humanitarian purposes.

4. Transnational nature and spillover effects – wartime cybercrime is rarely confined to the conflict zone. Its effects ripple outward, impacting neighboring countries and global systems. For example, malware originating in conflict zones can spread through international networks, compromising systems far from the original target.

The NotPetya ransomware, initially targeted at Ukraine, caused billions of dollars in damages worldwide, affecting multinational corporations and government systems.

Cybercrime in wartime cannot be viewed in isolation from the broader geopolitical context. It reflects the shifting paradigms of modern warfare, where digital dominance is as crucial as physical strength. The strategic use of cybercrime underscores the growing interdependence of digital and physical domains, demanding a comprehensive approach to understanding and addressing this evolving threat.

The classification of cybercrime schemes during wartime involves identifying distinct typologies based on their operational mechanisms and strategic objectives. These typologies highlight the adaptability of cybercriminals to the unique challenges of military conflicts.

1. Ransomware attacks have become a defining feature of wartime cybercrime. These attacks target essential services, encrypting data and demanding ransom payments to restore

access. During conflicts, ransomware is often deployed to disrupt healthcare, energy, and public administration systems, causing widespread societal and economic harm.

2. Phishing campaigns exploit the urgency and confusion of wartime to deceive individuals and organizations. By creating realistic but fraudulent messages related to emergencies or aid efforts, cybercriminals gain unauthorized access to sensitive information and critical systems.

3. Espionage and data breaches. Cyber espionage operations are a cornerstone of state-sponsored cybercrime during military conflicts. These attacks infiltrate government and military networks to extract intelligence that can influence military strategies and diplomatic negotiations.

4. Digital financial fraud – exploits weakened financial oversight in wartime economies. Fraudulent schemes target aid distribution systems, financial institutions, and digital payment platforms, redirecting resources intended for humanitarian and recovery efforts.

For a more comprehensive understanding of these typologies, refer to Table 2.1.

Table 2.1 – Approaches to the classification of types of cybercrimes in wartime

Appro-ach	Types of cybercrimes	Characteristic	War period	Post-war period
According to the motives and goals of the criminals	Financial Cybercrime	Attacks carried out in order to obtain financial benefits through fraud, theft of funds, theft of personal data, extortion and other methods of manipulation of funds.	**Ransomware (ransomware)** – attacks on government agencies, banking institutions, medical centers. The goal is to demand ransom.	Post-war fraud with recovery funds, the use of cyber tools to manipulate humanitarian aid.
	Ideological cybercrimes	Crimes aimed at propaganda, disinformation or influencing public opinion through cyberspace.	**Hacktivism** is attacks on political and social institutions to spread certain ideologies or to discredit governments	Continuation of propaganda through cyberspace, attacks on organizations engaged in the restoration of political order.
	Geopolitical cybercrimes	State-backed cyber operations with strategic objectives are often part of military operations or used to reconnoiter	**Cyberattacks on critical infrastructure** are attacks on energy, water and communication systems to destabilize the country.	**Cyber espionage and sabotage** are attacks on infrastructure related to recovery and economic

		and destabilize the situation.		stability after the war.
By attack methods	Malware (malware)	Using viruses, worms, Trojans, and other malware to gain access to systems and data.	**Ransomware (ransomware)** – freezing important files, stealing and storing data with a ransom demand.	The use of new types of malware to attack banking and recovery systems that manipulate data for financial gain.
	Phishing and social engineering	Attacks that are focused on deceiving users through fake sites, emails to gain access to confidential information.	Military phishing attacks to infiltrate senior government structures in an attempt to obtain intelligence.	Post-war use of phishing attacks to deceive in the processes of restoring the state structure, stealing information for manipulation with tenders and recovery.
	Attacks on suppliers and supply chains	Exploiting vulnerabilities in supply chains to infiltrate larger targets, manipulate data or infrastructure.	Attacks on suppliers to stop or block the supply of essential materials.	Use of cyber vulnerabilities in recovery processes to manipulate recovery contracts, technical assistance deliveries.
By scale and complexity	Ineffective cybercrimes	Simple attacks carried out by non-professional	Custom attacks, the use of simple phishing schemes to	Simple scams aimed at withdrawing funds from

		criminals or small groups.	extract information from small organizations or individuals.	government agencies through forged documents or distorted information.
	Highly professional cybercrimes	Cyber operations carried out by highly qualified organizations or government agencies, using modern technologies for complex attacks on critical systems.	Cyberattacks on government agencies, infrastructure in order to destabilize the situation and disable technical means of defense.	Sophisticated professional attacks on restored critical infrastructures (energy, transport systems) to obtain financial benefits.
By organization and actors of criminal activity	Individual cyber-criminals	Cybercrimes committed by individuals acting independently or under the influence of third parties.	Individual criminals can carry out phishing attacks, information theft or financial fraud over the Internet.	Theft of personal data for manipulation in recovery processes, deception when submitting documents or submitting false information.
	Organized criminal groups	Criminal organizations engaged in cybercrimes as part of large-scale operations.	International cybercriminal groups can carry out attacks on multiple government organizations	Post-war organized groups specializing in the use of cyber tools to speculate on regenerative

			or authorities in order to achieve strategic goals.	funds and programs.
According to legal characteristics	Cyberterrorism	The use of cybercrime to carry out terrorist acts involving attacks on national interests.	Attacks on energy and military systems to harm national security, attacks on energy networks and infrastructure of critical areas.	The use of terrorism in cyberspace to influence political or economic processes during recovery, attacks on new government systems.

Table 2.1 highlights the diverse approaches to classifying types of cybercrimes in wartime, showing how these evolve in the post-war context. The distinction by motives, attack methods, scale, and actors provides insights into designing targeted countermeasures.

Classifying organized and transnational cybercrime schemes during wartime requires an integrated approach that considers their functional, geographical, and organizational dimensions. These schemes often transcend national boundaries, making them difficult to detect and counteract.

1. Functional classification – cybercrime schemes can be categorized based on their operational objectives, such as operational disruption (e.g., ransomware), economic

exploitation (e.g., financial fraud), and information warfare (e.g., espionage and disinformation).

2. Geographical classification – cybercrime in wartime often reflects regional dynamics. Conflict zones experience high-intensity cyberattacks, while neighboring states face spillover effects. Advanced attacks may target global institutions with extensive digital networks.

3. Organizational classification – the actors involved in cybercrime include state-sponsored groups, independent criminal organizations, and collaborative networks. These actors often blur lines between criminal and military objectives.

Refer to Table 2.2 for a detailed breakdown.

Table 2.2 – Approaches to the classification of cybercrime schemes

Approach	**Characteristics of the approach**	**Types of cybercrime schemes**
By type of attack	Classification depending on the type of attack method used. Schemes are determined by the technical characteristics of criminal activity.	– **attacks due to vulnerabilities in software** (exploits, use of zero holes); – **attacks due to social engineering** (phishing, vishing); – **malware attacks** (extortion, trojans, worms).
By level of complexity and scale	Schemes are classified according to the level of complexity and scale of attacks. They are	– **simple schemes** (individual fraud through phishing, the use of viruses);

	determined based on the number of participants and the technical tools used.	– **complex schemes** (targeted attacks on infrastructure, complex ransomware); – **global schemes** (international cybercriminal networks)
By the level of organization of criminal activity	This approach is based on the definition of the organization of criminal activity: individual activities, small-scale groups or large criminal businesses.	– **individual schemes** (single criminals, phishing, data theft); – **organized criminal groups** (frauds that require coordination, scripts for stealing funds); – **transnational schemes** (multi-country criminal groups)
By type of object of attack	Classification depending on which part of the digital infrastructure or system is attacked.	– **infrastructure attacks** (energy, transport networks, water supply); – **attacks on personal data** (identity theft through phishing); – **attacks on financial institutions** (hacking of banking systems, fraud with payment cards)
By geographical orientation	Separation beyond the boundaries in which cybercrime is committed. This approach helps to distinguish between cybercrime that operates at the local, national or international levels.	– **local cybercrimes** (a limited area or individual institutions are attacked); – **national cybercrimes** (targeted attacks on government agencies); – **international cybercrimes** (global cybercriminal networks, transnational attacks).
By purpose	Classification of cybercrime schemes depending on the main goal of the criminal. It	– **fraud** (theft of money, data);

	can be theft, sabotage, blackmail, influencing political processes, etc.	– **sabotage** (damage or blocking of the functioning of infrastructure); – **blackmail** (ransomware through cyberattacks, theft of confidential information).
By tools and resources	Classification depending on what tools and resources are used to commit cybercrimes. These can be software, attack methods or material resources.	– **malware** (viruses, trojans, worms, ransomware); – **tools for identifying vulnerabilities** (exploits, automatic scanners); – **social engineering techniques** (phishing, manipulation of users).
By legal status	Division of cybercrime schemes on a legislative basis, depending on what laws are violated: crimes that pose a threat to national security or economic stability.	– **terrorist cybercrimes** (attacks on critical infrastructure to destabilize the state); – **financial crimes** (fraud with payment systems, theft of bank data); – **intellectual crimes** (copyright infringement through software, cyber espionage)
By impact on goals	Distribution of schemes depending on the scale of impact on the target system or infrastructure. Crimes can be aimed at small-scale attacks or on large global systems.	– **local attacks** (phishing, personal violations); – **large-scale attacks** (cyberattacks on government or large organizations); – **global cybercrimes** (international cyberattacks, attacks on multinational corporations).

Table 2.2 illustrates the systematic approaches to categorizing cybercrime schemes. It underscores the importance

of understanding the types of attacks, organizational levels, and geographical orientations to develop targeted counter-strategies.

Cross-border cybercrime schemes during wartime reflect the interconnected nature of global digital systems. These crimes exploit the lack of clear jurisdiction in cyberspace, creating challenges for law enforcement and international cooperation.

1. Cross-border ransomware campaigns – these campaigns often target multinational corporations and international aid organizations, exploiting their expansive digital infrastructure. NotPetya (2017) – initially targeting Ukraine, this ransomware spread globally, affecting companies such as Maersk and costing billions in damages.

2. International espionage networks – cyber espionage operations often involve state-sponsored actors targeting foreign governments and corporations to gain strategic advantages. During the Afghanistan conflict, cyber espionage targeted NATO allies, extracting sensitive military data and compromising coalition operations.

3. Cryptocurrency laundering – the use of cryptocurrencies for laundering illicit funds has become a hallmark of cross-border cybercrime in wartime. These schemes exploit the anonymity and decentralization of digital currencies. Syria (2016)**:** militants used Bitcoin to fund operations,

bypassing traditional financial systems and evading international sanctions.

2.3. Clustering academic research on cybersecurity and cybercrime in wartime: branching and concentration of research networks [7]

Cluster analysis of scientific research is a critical approach to understanding the structure, dynamics, and key themes within a research domain. In the context of cybersecurity during wartime, this method allows for the identification of dominant areas of study, cross-sectoral connections, and potential gaps in knowledge. Such analysis provides insights into thematic focus, geographic distribution, institutional affiliations, and the evolution of key research areas. It also informs strategies for enhancing interdisciplinary collaboration and addressing emerging challenges in cybersecurity.

The first step in this cluster analysis involved a contextual review of scientific literature sourced from Scopus and WOS databases.

[7] This chapter was prepared as part of a research project 0124U000550

The selected keywords and combinations were chosen to capture a broad spectrum of studies addressing technological, strategic, and geopolitical dimensions of cyber threats in conflict settings. The following queries formed the basis for the analysis:

1. Military Conflict Combined AND Cybercrime (search focused on exploring the intersection of military conflicts and cybercriminal activities, highlighting the role of organized cybercrime during wars).

2. Military Conflict AND Cybersecurity (examined the role of cybersecurity strategies in mitigating risks posed by cyberattacks during military engagements).

3. Wartime Technology AND Security (investigated the application of advanced technologies to enhance security measures during wartime scenarios).

4. Cybercrime AND War (explored broader implications of cybercrime in the context of military conflicts and war-related vulnerabilities).

5. Cybersecurity AND War (studied the strategies and measures adopted to protect critical infrastructure and national interests during wartime).

These queries provided a structured framework for identifying relevant studies that inform the clustering of academic achievements in this domain. The search results enabled the identification of key thematic areas, facilitating the

subsequent clustering and analysis of research networks and scientific landscapes.

The cluster analysis results, visualized in Figure 2.1, reveal the primary clusters and their interconnections.

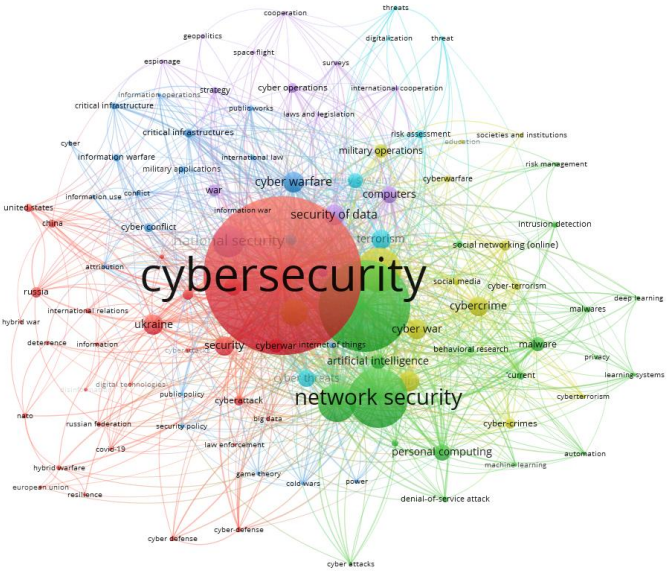

Figure 2.1 – Network visualization of cybersecurity and cybercrime research clusters

Each cluster represents a distinct thematic focus in the field of cybersecurity and cybercrime during wartime. Table 2.3 provides a detailed description of the six main clusters identified through the analysis.

The analysis reveals a multifaceted and interdisciplinary structure of research on cybersecurity and cybercrime. The red cluster dominates in terms of publications, highlighting the critical importance of protecting infrastructure and implementing effective regulatory frameworks.

Table 2.3 – Contextual clustering of research on cybersecurity and cybercrime in wartime

Cluster	Primary theme	Key terms	Characteristics
Cluster 1 (Red)	Cybersecurity and Critical Infrastructure	Cybersecurity, critical infrastructure, cyber operations, cyber defense, laws and legislation	Focuses on protecting critical infrastructures, regulatory frameworks, and operational cybersecurity measures.
Cluster 2 (Green)	Network Security	Network security, intrusion detection, malware, social engineering, artificial intelligence	Examines threat detection technologies, the use of AI, and measures to prevent cyberattacks.
Cluster 3 (Blue)	Cybercrime	Cybercrime, cyber terrorism, behavior research, denial-of-service attack	Explores cybercrime schemes, including terrorism and behavioral aspects of cybercriminal activities.
Cluster 4 (Purple)	Military Operations and Geopolitics	Military operations, hybrid war, deterrence, resilience, Russian Federation, Ukraine	Investigates hybrid wars, the geopolitical impact of cyber threats, and

			implications for international relations.
Cluster 5 (Yellow)	Data Security	Security of data, privacy, encryption, digital resilience	Studies focused on data security, privacy issues, and the resilience of digital systems to threats.
Cluster 6 (Orange)	Social Aspects of Cybersecurity	Social networking, public policy, online safety, human factors	Highlights the intersection of cybersecurity with social factors, public policies, and user protection.

The green and blue clusters emphasize technical aspects, such as network security and cybercrime dynamics, while the purple cluster illustrates the intersection of cyber threats with military operations and geopolitical factors. The yellow and orange clusters address data security and social dimensions, showcasing the diversity of research interests.

Following the network analysis of key themes and clusters in cybersecurity and cybercrime research, the next logical step is to conduct a contextual-temporal analysis. This method enables the exploration of how research focus areas evolve over time and how dominant themes interconnect across temporal dimensions. This approach is critical for understanding the historical trajectory and emerging trends in cybersecurity studies, particularly during wartime and post-war periods.

The visualization in Figure 2.2 highlights the density of connections between dominant keywords and thematic clusters over a specific time period. It provides a foundation for identifying temporal patterns and shifts in academic focus.

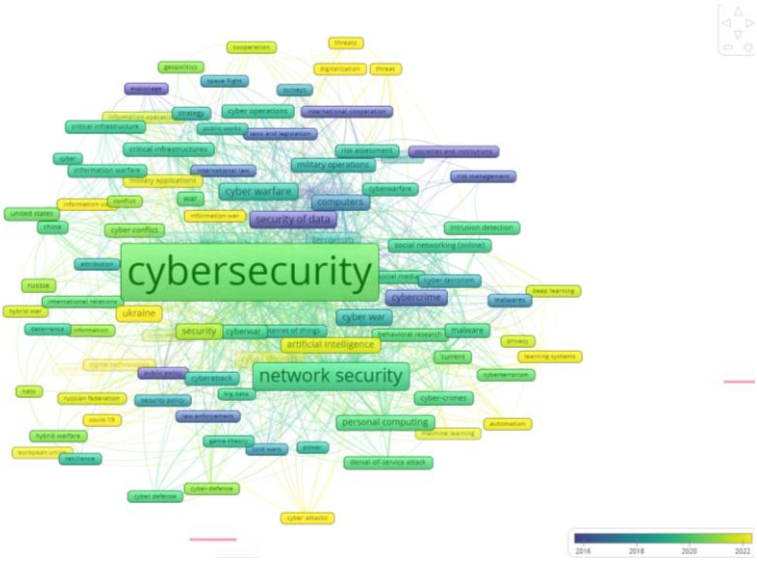

Figure 2.2 – Contextual-temporal analysis of cybersecurity and cybercrime research clusters

The findings of the contextual-temporal clustering, summarized in the table 2.4, provide insights into how cybersecurity research has transitioned from foundational themes to more sophisticated and integrated approaches.

The contextual-temporal analysis underscores a clear progression in cybersecurity research. Before 2016, studies predominantly addressed foundational concepts such as national

security and basic cyber threats. Post-2016, the focus shifted to advanced technologies, hybrid threats, and automation, reflecting the growing complexity of cyber operations and defense mechanisms.

Table 2.4 – Contextual-temporal clustering of research on cybersecurity and cybercrime in wartime

Time period	Cluster name	Dominant keywords	Key characteristics
Before 2016	Cyber Warfare & National Security	Cyber warfare, national security, espionage	Focused on military applications, geopolitical tensions, and state-sponsored cyber operations.
	Information Security	Information use conflict, critical infrastructure	Emphasis on securing communication systems and protecting infrastructure from sabotage.
	Social Engineering Threats	Social engineering, phishing, malware	Research concentrated on individual-level attacks and basic malware defense.
2016–2018	Hybrid Threats	Hybrid war, deterrence, resilience	Emergence of hybrid threats combining traditional military actions with cyber strategies.
	Data Security & AI	Artificial intelligence, machine learning, security of data	Integration of AI-driven tools for monitoring and securing sensitive information.
	Cyber Defense Systems	NATO, cyber defense, military operations	Development of large-scale cyber defense strategies by intergovernmental organizations and alliances.

2019–2024	Network Security & Automation	Network security, cybersecurity, automation	Expanded focus on automating cybersecurity responses and securing network infrastructures.
	Digital Resilience	Digital technologies, cyber resilience, EU regulations	Shift towards building long-term resilience through regional and global regulatory frameworks.
	Cybercrime & Critical Systems	Cybercrime, malware, intrusion detection	Advanced research into detecting and mitigating threats to critical systems such as healthcare and financial services.

Future research should continue to analyze the intersection of these clusters while incorporating temporal fluctuations in research emphasis.

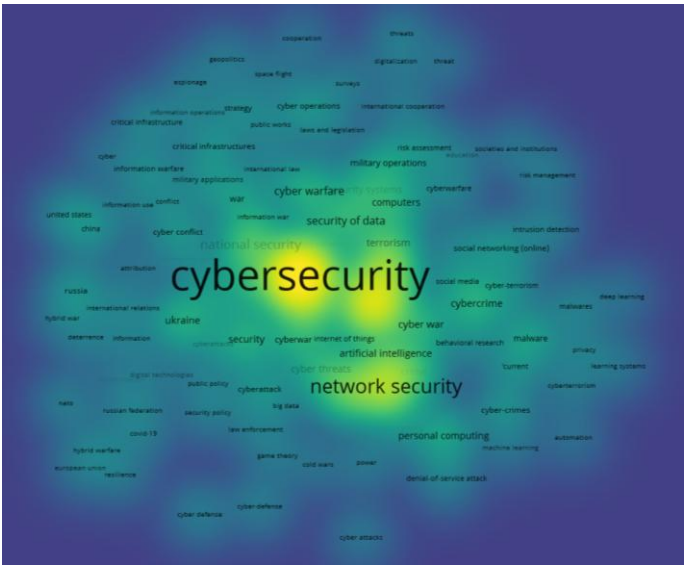

Figure 2.3 – Density visualization of cybersecurity and cybercrime research themes during wartime

The provided density visualization represents the intensity and frequency of interconnected research themes in the field of cybersecurity, with particular emphasis on wartime and related topics. The color gradient indicates the density of keywords, where warmer colors (yellow) signify areas of concentrated research activity, and cooler colors (blue) represent less intensive clusters of exploration.

1. Central keywords:

– the term "cybersecurity" occupies the most prominent position, highlighted in bright yellow, reflecting its centrality and high frequency in the dataset;

– closely related terms such as "network security", "cyber warfare", and "national security" are adjacent, indicating a strong thematic correlation;

2. Substantial research focus areas:

– cyber warfare: frequently associated with terms like "military applications," "security of data," and "critical infrastructures," reflecting its importance in wartime scenarios;

– network security: linked to practical implementations and threat mitigation, including "malware," "intrusion detection," and "denial-of-service attacks".

– artificial intelligence: positioned near cybersecurity, suggesting its growing role in predictive threat analysis and automated defense mechanisms.

3. Emerging topics:

– hybrid warfare and resilience: emerging as significant themes in the context of modern geopolitical conflicts, particularly in regions like Ukraine;

– social media and cyberterrorism: highlighting the increasing intersection of cybersecurity with public communication platforms and terrorism.

4. Geographical and contextual terms:

– countries like Ukraine, Russia, and global entities such as NATO are evident, underscoring the geopolitical dimensions of cybersecurity research.

5. Cross-sectoral research:

– connections to "critical infrastructure," "law enforcement," and "public policy" indicate interdisciplinary approaches to addressing cyber threats during conflicts.

6. Temporal evolution:

– the density of research activity (warmer regions) is more concentrated around concepts directly linked to active conflict periods (e.g., "war," "cyber defense"), reflecting the urgency of addressing these themes during wartime.

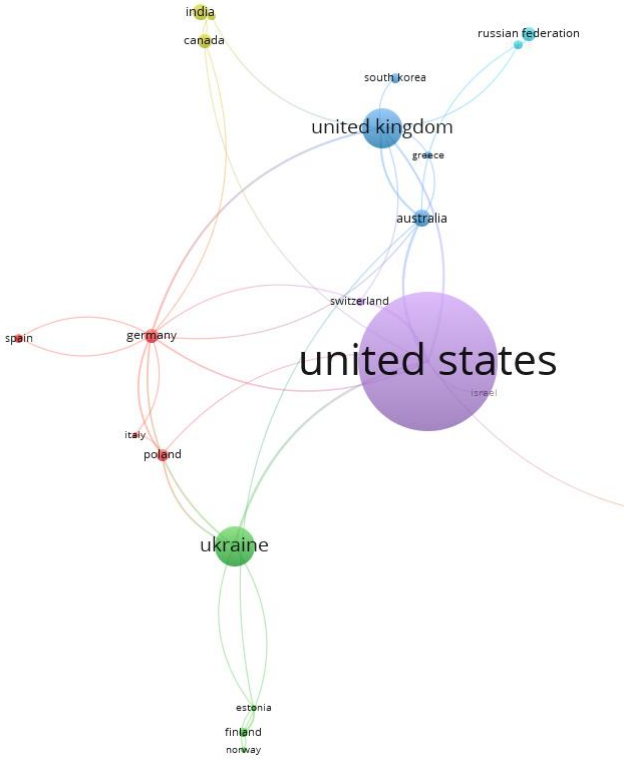

Figure 2.4 – Network visualization of international scientific cooperation on cybersecurity and cybercrime in wartime

The provided Figure 2.4 highlights the international collaboration in cybersecurity and cybercrime research during wartime, with an emphasis on geographic affiliations of researchers and institutions. The size of the nodes represents the volume of publications, while the thickness of the connecting lines indicates the strength of collaborative relationships.

1. Dominant players:

–the United States is the largest node, indicating its leading role in cybersecurity research. The country collaborates extensively with other nations, as shown by the numerous links connecting it to countries such as the United Kingdom, Germany, and Australia;

–Ukraine emerges as a significant node in the context of wartime cybersecurity, reflecting its unique challenges and contributions during the ongoing conflict.

2. Regional clusters:

–a strong European cluster includes Germany, Poland, Italy, and Spain, showcasing active regional collaboration. This grouping highlights shared interests in cybersecurity policies and defense mechanisms within the EU;

–United Kingdom serves as a bridge between North America (United States and Canada) and Europe, playing a pivotal role in facilitating international research networks.

3. Emerging nations:

–countries such as India, South Korea, and Nigeria are present, reflecting growing contributions to global cybersecurity research. Their links to major players like the United States signify increasing integration into the broader research landscape.

4. Geopolitical relevance:

–Connections between Ukraine, Russia, and NATO countries such as Norway, Finland, and Estonia underscore the geopolitical dimensions of cybersecurity research. These links highlight how wartime realities influence research priorities and collaboration.

5. Collaboration strength:

–the thicker lines between the United States and the United Kingdom indicate a high level of joint research output, followed by notable collaborations between the United States and Germany, as well as between Ukraine and neighboring European countries.

This visualization underscores the critical role of international collaboration in addressing the complexities of cybersecurity during wartime. The prominence of certain countries reflects their investment in research and their response to geopolitical challenges. Additionally, the visualization illustrates how regional and global partnerships can enhance knowledge-sharing and innovation in tackling cybercrime and related threats.

Spatio-temporal network visualization (figure 2.5) highlights the geographic and temporal dimensions of cybersecurity and cybercrime research during wartime.

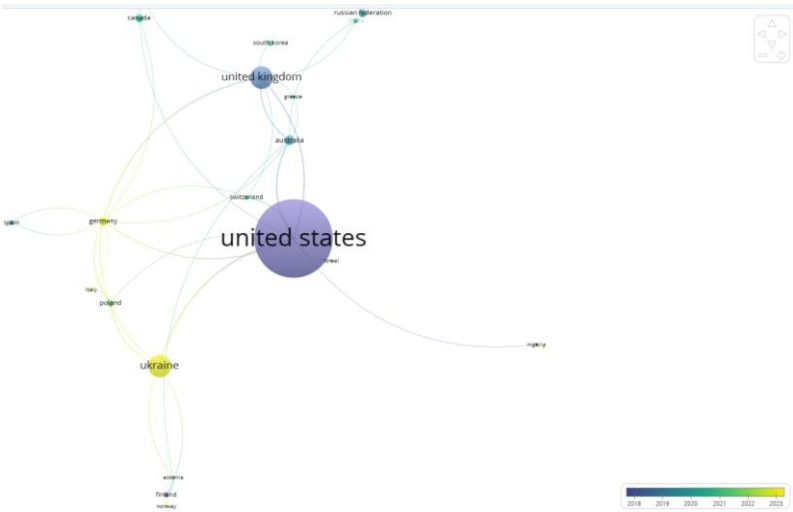

Figure 2.5 – Spatial and temporal visualisation of international scientific cooperation on cybersecurity and cybercrime in wartime

The nodes represent countries, with the size indicating the volume of academic contributions (e.g., number of publications). The links between nodes illustrate collaborative relationships, with thicker lines representing stronger academic partnerships. The color gradient reflects the average publication year, providing insight into when specific regions became active in cybersecurity research.

Table 2.3 – Spatio-temporal clustering of research on cybersecurity and cybercrime in wartime

Cluster	Key Countries	Temporal Trends	Research Focus
Cluster 1	United States, United Kingdom, Germany	Continuous activity since early 2000s	Advanced cybersecurity strategies, AI applications, and policy frameworks.
Cluster 2	Ukraine, Poland, Finland	Accelerated activity post-2014	Countering cyber espionage, protecting critical infrastructure.
Cluster 3	India, South Korea	Emerging in 2018–2023	AI-driven cybersecurity, hybrid warfare.
Cluster 4	Nigeria	Recent research focus	Addressing cybercrime in developing economies.

This spatio-temporal analysis underscores the evolution of cybersecurity research across regions and time. While traditional leaders like the United States and Western Europe have sustained contributions, Ukraine and its neighbors have emerged as critical players in response to evolving wartime threats. Emerging economies such as India and Nigeria indicate a broader global recognition of cybersecurity's role in maintaining stability during conflicts. These patterns highlight a growing convergence of regional and global efforts in combating cybercrime and securing critical infrastructure.

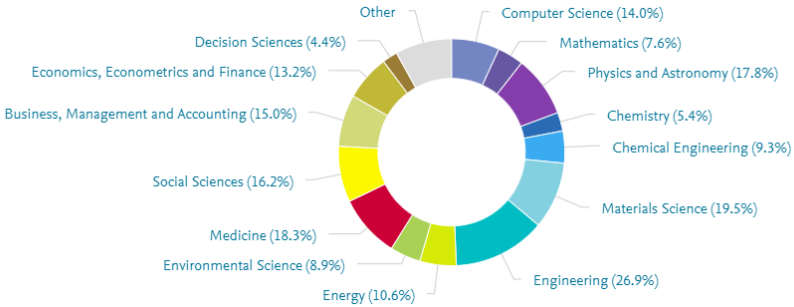

Figure 2.6 – Network visualization of international scientific cooperation on cybersecurity and cybercrime in wartime

Figure 2.6 presents the distribution of scientific publications by subject area, emphasizing the multidisciplinary nature of research in cybersecurity and cybercrime during wartime. Each segment of the chart represents a subject area, showing its proportional contribution to the overall research output.

1. Dominant fields:

– engineering (26.9%) holds the largest share, reflecting the technical focus of cybersecurity research, particularly on designing resilient systems and critical infrastructure protection during military conflicts;

– materials science (19.5%) and medicine (18.3%) indicate the role of cybersecurity in healthcare systems and

emerging technologies that rely on secure materials and platforms.

2. Cross-disciplinary contributions:

– social sciences (16.2%) demonstrates the importance of studying the societal and behavioral aspects of cybercrime, including the implications of disinformation campaigns and public awareness;

– business, management, and accounting (15.0%) highlights the economic dimension of cybersecurity, focusing on fraud prevention, financial risk management, and anti-corruption strategies.

3. Specialized areas:

– computer science (14.0%) underlines the centrality of algorithms, artificial intelligence, and software solutions in tackling cyber threats;

– economics, econometrics, and finance (13.2%) connects the financial implications of cybercrime with broader economic stability.

4. Environmental and energy focus:

– environmental science (8.9%) and energy (10.6%) point to the growing need to secure energy grids and environmental data systems from cyberattacks, especially during wartime.

5. Emerging disciplines:

– physics and astronomy (17.8%), mathematics (7.6%), and decision sciences (4.4%) contribute through advanced modeling, cryptography, and decision-making frameworks for combating cybercrime.

In general, the chart demonstrates the importance of interdisciplinary approaches to address cybercrime effectively. By leveraging insights from diverse fields, researchers and policymakers can develop comprehensive strategies to strengthen resilience against cyber threats during military conflicts. This holistic view is critical for crafting robust cybersecurity policies that protect both critical infrastructure and societal well-being.

The critical role of cybersecurity and the increasing prevalence of cybercrime during wartime have made these topics a focal point for researchers worldwide. This review synthesizes recent academic achievements, mapping the branching or concentration of research networks in this field.

Key themes in the literature:

1. **Cybersecurity governance and policies**. Cybersecurity governance during conflicts has been explored through various lenses. Slupska (2021) discusses the use of generative metaphors in shaping cybersecurity governance, emphasizing how war metaphors influence policy development. Kelemen (2023) highlights the impact of the Russian-Ukrainian

hybrid war on European Union cybersecurity regulations, illustrating the rapid policy evolution triggered by external threats.

Bygrave (2025) provides a comprehensive account of the emergence of EU cybersecurity law, identifying challenges in policy implementation due to jurisdictional overlaps and regulatory complexities. Antonio (2024) examines disparities in North American cybersecurity policies, focusing on cooperative challenges between Mexico, the United States, and Canada.

2. **Cybercrime dynamics in wartime**. The dynamics of cybercrime during wartime are a critical area of focus. Normatovich and Boboyorov (2021) delve into the intersection of cybersecurity and information warfare, highlighting how cyberattacks are weaponized during conflicts. Vilpišauskas (2024) analyzes the effects of Russian cyberattacks on Lithuania's cybersecurity policies, showcasing the transformative impact of persistent threats.

Harknett et al. (2010) propose a shift from traditional deterrence strategies to proactive war-fighting measures in national cybersecurity. Similarly, Pattison (2020) examines the ethical implications of offensive cybersecurity measures by private entities, emphasizing the balance between defense and aggression in cyberspace.

3. **Cybersecurity education and awareness.** Terepyshchyi and Kostenko (2022) map the landscape of cybersecurity education during the war in Ukraine, highlighting the rapid adaptation of educational frameworks to address emerging threats. Anvik et al. (2019) and Tareque et al. (2024) introduce game-based learning approaches to teaching cybersecurity concepts, demonstrating innovative methods for building cybersecurity awareness and skills.

de Bruijn and Janssen (2017) emphasize the need for evidence-based framing strategies to enhance cybersecurity awareness, advocating for targeted campaigns that resonate with diverse stakeholders.

4. **Technological innovations and cybersecurity.** Technological advancements play a pivotal role in strengthening wartime cybersecurity. Park and Lee (2020) propose a Hyperledger blockchain design for secure information sharing, showcasing its potential in protecting national cybersecurity data. Park et al. (2018) evaluate South Korea's cybersecurity policies, recommending systemic upgrades to address evolving threats.

Hough and Gross (2019) discuss the invisible nature of cyber threats, emphasizing the need for advanced diagnostic tools to detect and mitigate cybercrime effectively.

5. **Regional and international cooperation**. International collaboration is critical in addressing cross-border cyber threats. Lewis (2021) explores bilateral negotiations for cybersecurity cooperation, highlighting the complexities of fostering trust between nations. Normatovich and Boboyorov (2021) stress the importance of international partnerships in combating information warfare, particularly during large-scale conflicts.

Pattison (2020) and Vilpišauskas (2024) underscore the role of shared policies and collective security measures in mitigating cyber threats, advocating for unified global strategies.

Despite significant advancements, the following gaps persist:

– longitudinal analyses: few studies provide insights into the long-term evolution of cybersecurity strategies and policies post-conflict.

– technological adaptation: limited research addresses the integration of emerging technologies, such as artificial intelligence, in wartime cybersecurity frameworks.

– cross-cultural studies: the global diversity in cybersecurity governance approaches remains underexplored.

– ethical implications: further exploration of the ethical challenges in offensive and defensive cybersecurity measures is needed.

Future studies should:

1. Expand interdisciplinary approaches: integrate perspectives from political science, technology, and ethics to address the multifaceted nature of cybersecurity in wartime.

2. Focus on emerging technologies: investigate the role of AI, machine learning, and blockchain in enhancing wartime cybersecurity measures.

3. Enhance global collaboration: develop frameworks for international cooperation, addressing legal and jurisdictional challenges.

4. Promote educational innovation: explore novel methods for building cybersecurity awareness and resilience, particularly in conflict-prone regions.

The academic exploration of cybersecurity and cybercrime in wartime highlights significant achievements and critical gaps. Addressing these challenges through global collaboration, technological innovation, and interdisciplinary research will be crucial in enhancing cybersecurity resilience during and after conflicts.

Conclusions to Chapter 2

The evolving nature of modern warfare has placed cybersecurity at the forefront of national security and economic resilience, especially during periods of conflict. Chapter 2

provided an extensive examination of cybersecurity challenges and transnational cybercrime in wartime, elucidating foundational concepts, practical implications, and academic advancements in the field. The insights derived from this analysis underscore the multi-faceted nature of cyber threats, the sophistication of organized crime networks, and the critical need for a collaborative and research-driven approach to cybersecurity.

The foundational exploration of cybersecurity during wartime highlighted the dual vulnerabilities faced by nations—both in physical and cyber domains. Modern warfare has extended beyond battlefields into cyberspace, where adversaries exploit technological infrastructures, disrupt critical services, and target economic stability. Wartime conditions amplify these threats, creating an environment where cybercriminals thrive, exploiting weak governance, fractured communication, and inadequate technological readiness.

The analysis underscored the pressing need for robust cybersecurity frameworks tailored to the wartime context. Critical challenges include defending critical infrastructure from cyberattacks, addressing cross-border complexities in transnational cybercrime, and combating the proliferation of new and innovative attack vectors such as ransomware, phishing, and cyber espionage. These issues demand not only

immediate operational responses but also strategic long-term planning and investment in resilient systems.

The typologies of organized and transnational cybercrime schemes presented in this chapter revealed the intricate and adaptive nature of cybercriminal operations. From ransomware attacks targeting healthcare and government institutions to sophisticated phishing campaigns designed to extract intelligence or financial gains, the schemes of cybercrime demonstrate a high degree of organization, technological expertise, and alignment with geopolitical objectives.

The analysis identified critical distinctions in the characteristics of wartime and post-war cybercrime schemes. For instance:

– Wartime cybercrime: focused on destabilizing critical infrastructure, disrupting supply chains, and spreading misinformation for strategic advantages.

– Post-war cybercrime: oriented towards exploiting recovery efforts, manipulating aid distribution, and engaging in financial fraud through cyber-enabled means.

Furthermore, the classification frameworks provided a systematic understanding of these schemes, categorized by attack methods, motives, organization levels, and geographic scope. This categorization not only facilitates a deeper understanding of cybercrime dynamics but also provides

actionable insights for policymakers and law enforcement agencies in designing targeted countermeasures.

The exploration of the academic landscape surrounding cybersecurity and cybercrime in wartime underscored the interdisciplinary and global nature of this field. Using advanced bibliometric techniques and clustering analysis, the chapter mapped the dominant research areas, thematic intersections, and key contributors to the discourse.

Key findings include:

– Dominant research areas: cybersecurity for critical infrastructure, cyber defense in military operations, and the role of AI and blockchain in combating cybercrime emerged as focal points of scholarly attention.

– Cross-Sectoral Research: The intersection of cybersecurity with fields such as international law, political science, and economics highlights the need for multi-disciplinary approaches to address cyber threats comprehensively.

– Global contributions: countries such as the United States, United Kingdom, and Ukraine have emerged as significant contributors to research, reflecting their experiences and investments in addressing wartime cyber threats.

The clustering analysis further revealed dense linkages between academic institutions, underscoring the importance of

international collaboration in advancing cybersecurity research and translating academic findings into practical solutions.

The overarching findings of Chapter 2 underscore the complexity and criticality of addressing cybersecurity and cybercrime in wartime. Key implications include:

1. Need for tailored cybersecurity frameworks: wartime scenarios demand specialized approaches that account for the unique challenges posed by transnational cybercrime and the vulnerabilities of critical infrastructure.

2. Importance of research and collaboration: Academic advancements and cross-sectoral collaborations provide the foundation for innovative solutions, enhanced threat intelligence, and more effective policy interventions.

3. Integration of advanced technologies: the deployment of AI, blockchain, and advanced analytics is vital for detecting, mitigating, and preventing cybercrime in both wartime and post-war contexts.

4. Global and regional partnerships: strengthened international cooperation is essential to combat transnational cybercrime, share intelligence, and harmonize cybersecurity standards.

In conclusion, this chapter has provided a comprehensive overview of the scientific, practical, and policy dimensions of cybersecurity and transnational cybercrime during wartime. The

findings underscore that the digital battlefield is now an integral component of modern conflicts, necessitating a proactive, collaborative, and technology-driven approach. By leveraging academic insights, fostering international partnerships, and investing in cutting-edge technologies, nations can better safeguard their digital ecosystems, protect critical infrastructures, and ensure economic resilience in the face of wartime cyber threats. This chapter sets the foundation for further exploration of strategies and frameworks to strengthen cybersecurity in an increasingly interconnected and conflict-prone world.

CHAPTER 3. CYBERSECURITY AND DIGITAL TRANSFORMATION OF THE WAR AND POST-WAR ECONOMY: FIGHTING CYBERCRIME, FINANCIAL FRAUD, CORRUPTION AND THE SHADOW SECTOR

3.1 Cybersecurity and cybercrime in wartime: insights from countries engaged in military conflict[8]

The proliferation of digital technologies has made cyberspace an integral component of national security, economic stability, and societal resilience. However, during wartime, the fragility of digital infrastructure becomes a strategic vulnerability. Cybercrime during military conflicts has evolved beyond opportunistic financial schemes, transforming into a tool for destabilization, espionage, and disruption of critical infrastructure. Nations embroiled in conflicts, particularly those with limited resources, often find themselves at the intersection of digital warfare and organized cybercrime, facing threats that undermine their sovereignty and operational stability.

8 This chapter was prepared as part of a research project 0124U000550

One of the most damaging forms of cybercrime during military conflicts is the targeted disruption of critical infrastructure, including energy grids, healthcare systems, and communication networks (Table 3.1).

Table 3.1 – Cyberattacks on critical infrastructure during wartime

Country	Primary target	Type of attack	Impact
Ukraine	Energy, healthcare	Malware (BlackEnergy, HermeticWiper)	Power outages, disruption of emergency services
Georgia	Government communication	DDoS attacks	Loss of access to critical government information
Syria	Healthcare systems	Ransomware	Delays in humanitarian aid and disruption of medical services

These attacks aim to paralyze essential services and sow chaos, often complementing physical warfare:

– Ukraine (2015–2023) has been a consistent target of cyberattacks since the annexation of Crimea in 2014. The 2015 BlackEnergy malware attack marked a turning point, disrupting power grids and affecting 230,000 households. During the full-scale invasion in 2022, attacks such as HermeticWiper targeted healthcare facilities, further stressing Ukraine's already strained emergency services.

– Georgia (2008). During the Russo-Georgian War, cyberattacks on government websites and critical communication systems paralyzed the nation's ability to disseminate information, creating confusion and disrupting military coordination.

– Syria (2011–2023). In the ongoing Syrian conflict, ransomware attacks on healthcare providers have impeded humanitarian aid, delaying critical services and worsening the humanitarian crisis.

Financial systems during wartime are highly susceptible to cyber exploitation. Cybercriminals take advantage of weakened regulatory oversight to conduct money laundering, fraud, and theft, often funding further criminal or militant activities:

– Afghanistan (2001–2021). During the U.S.-led war in Afghanistan, digital payment systems were exploited for laundering money. Weak oversight in a war-torn economy facilitated the illicit flow of funds, much of which was redirected to sustain insurgencies.

– Yemen (2015–2023). In Yemen, fraudulent activities in the distribution of humanitarian aid have become a recurring problem. Cybercriminals manipulate digital records to divert funds, undermining relief efforts and deepening economic instability.

– Nigeria (2009–Present). The ongoing Boko Haram insurgency in Nigeria has seen the use of cyber-enabled fraud to fund operations. Social engineering schemes and online scams have exploited global charities and individuals seeking to aid displaced populations.

Espionage remains a central feature of cybercrime during conflicts, with attackers targeting government, military, and corporate data to gain strategic advantages:

– Armenia-Azerbaijan (2020). During the Nagorno-Karabakh conflict, phishing campaigns and spyware were employed to infiltrate military communication systems, gathering intelligence on troop movements and battle strategies.

– United States (2003–2021). Cyberattacks during the Iraq and Afghanistan wars frequently targeted U.S. contractors and agencies. State-sponsored actors used these attacks to access sensitive military plans and logistical data.

Disinformation campaigns have become a hallmark of modern conflicts, using digital platforms to manipulate public opinion, destabilize governance, and influence international perceptions:

– Russia-Ukraine Conflict (2014–Present). Russia's extensive use of disinformation campaigns has targeted both domestic and international audiences. Social media platforms

were weaponized to spread propaganda, create divisions, and undermine trust in Ukraine's leadership.

– Middle East (2011–2023). In Syria, ISIS leveraged social media to disseminate propaganda and recruit fighters globally. Disinformation also served as a tool to delegitimize opposing factions.

The manifestations of cybercrime vary across regions, influenced by the geopolitical and economic contexts of each conflict (Table 3.2).

Table 3.2 – Comparative impact of cybercrime across regions

Region	**Key cybercrime Issue**	**Impact**	**Response**
Sub-Saharan Africa	Financial fraud	Exploitation of weak regulatory systems	Increased reliance on international law enforcement
Eastern Europe	Infrastructure attacks	Disruption of critical energy and healthcare services	International partnerships with NATO and EU
Middle East	Cryptocurrency laundering	Funding of militant activities	Limited regional coordination

Table 3.2 shows that:

–Sub-Saharan Africa: weak governance and limited technological infrastructure make this region particularly vulnerable to financial fraud and phishing schemes.

–Eastern Europe: Ukraine's resilience against cyberattacks showcases the importance of international support and local innovation. Collaborative efforts with NATO and private cybersecurity firms have strengthened Ukraine's defenses.

– Middle East: prolonged conflicts in Yemen and Syria have created fertile ground for ransomware attacks and cryptocurrency-based money laundering, leveraging the chaos and lack of oversight in these war-torn economies.

Table 3.3 provides an overview of the economic losses attributed to cybercrime in wartime economies.

Table 3.3 – Economic impact of cybercrime in wartime economies (Estimates, 2020–2023)

Country	**Conflict Period**	**Estimated Loss ($ Billion)**	**Primary Sources of Loss**
Ukraine	2014-2023	10.5	Financial fraud, ransomware, phishing scams
Syria	2011-2023	2.3	Illicit cryptocurrency mining, data theft
Afghanistan	2001-2021	1.7	Smuggling via digital payment systems
Yemen	2015-2023	0.9	Black market operations and online scams
Sub-Saharan Africa	2015-2023	1.5	Fraudulent humanitarian aid transactions

The financial damage ranges from ransomware and phishing scams in Ukraine to illicit cryptocurrency mining in Syria. The table emphasizes the significant burden that cybercrime places on economies already strained by conflict. For example, Ukraine's estimated loss of $10.5 billion reflects the extensive use of cyberattacks as a strategic tool in the ongoing conflict, while losses in sub-Saharan Africa reveal the exploitation of weak regulatory systems and humanitarian vulnerabilities. Table 3.4 categorizes the primary motivations driving transnational cybercrime during wartime.

Table 3.4 – Key motivations for transnational cybercrime during wartime

Motivation	Examples	Implications
Financial gain	Cryptocurrency theft, ransomware	Funds illicit operations, undermines economies.
Espionage	Data breaches in government and military systems	Loss of strategic and national security information.
Destabilization of governance	Attacks on electoral systems, disinformation campaigns	Weakens public trust, promotes instability.
Tactical military advantage	Disruption of logistics, communication, and energy supplies	Amplifies physical conflict outcomes.
Influence on public sentiment	Propagation of propaganda and fake news through digital platforms	Alters public perception, erodes morale.

It highlights how cybercriminal activities extend beyond financial gain to include espionage, political destabilization, and influencing public sentiment. For instance, disinformation campaigns aimed at altering public opinion have become a key tool in hybrid warfare, while ransomware attacks disrupt critical infrastructure, directly impacting military and civilian operations.

The analysis of cybercrime during wartime reveals its pervasive and multifaceted nature. From critical infrastructure attacks in Ukraine and Georgia to financial exploitation in Afghanistan and Yemen, cybercriminals exploit the vulnerabilities of nations under duress. Moreover, the global interconnectedness of cybercrime necessitates international cooperation and the sharing of best practices.

The experiences of nations like Estonia and Ukraine demonstrate the potential for resilience through innovative cybersecurity strategies and partnerships. Conversely, regions with weaker governance structures, such as Sub-Saharan Africa, continue to struggle against cybercrime, emphasizing the need for targeted international support. This analysis underscores the urgent need for comprehensive cybersecurity frameworks tailored to the unique challenges of wartime.

3.2 Implications of cybercrime on economic and national security[9]

Cybercrime during wartime presents a multifaceted threat to both economic stability and national security. By exploiting digital vulnerabilities, cybercriminals disrupt critical infrastructure, divert financial resources, and undermine trust in institutions, creating a cascade of economic challenges that exacerbate the pre-existing vulnerabilities of nations engaged in conflict. This section explores the ways in which cybercrime contributes to economic destabilization and its broader implications for national security.

Cyberattacks on critical infrastructure, such as energy grids, financial systems, and healthcare services, have immediate and far-reaching economic consequences. These attacks amplify the operational challenges faced by nations in conflict and lead to significant economic losses:

1. **Energy infrastructure**. Attacks targeting power grids disrupt industrial production, public utilities, and essential services, leading to financial losses across multiple sectors. For example, the 2015 BlackEnergy attack on Ukraine's power grid

9 This chapter was prepared as part of a research project 0124U000544

caused widespread outages, halting economic activity in affected regions and requiring costly restoration efforts.

2. **Healthcare systems**. Cyberattacks on hospitals and emergency services delay medical care and increase mortality rates, placing additional strain on economies through loss of productivity and increased healthcare expenditures. The HermeticWiper attack on Ukrainian hospitals during the 2022 conflict demonstrated how cybercrime can cripple critical public services.

3. **Communication networks**. Disruptions to communication systems hinder coordination between government agencies, businesses, and citizens, reducing efficiency in emergency responses and economic recovery efforts. Such attacks also damage investor confidence, discouraging foreign direct investment (FDI).

Cybercrime diverts financial resources from productive economic activities to addressing fraud, ransomware payments, and the restoration of compromised systems. This diversion has both direct and indirect impacts on economic growth and stability.

1.**Fraudulent activities**. Financial fraud during wartime often involves the misappropriation of funds intended for humanitarian aid or reconstruction. In Yemen, cybercriminals exploited digital payment systems to siphon funds from

international aid, depriving vulnerable populations of critical resources. The misuse of stolen financial data further burdens financial institutions with fraud mitigation costs, reducing their capacity to lend and support economic recovery.

2.**Ransomware attacks**. Ransom payments drain national resources while emboldening cybercriminal networks. The WannaCry ransomware attack in Syria disrupted financial operations and forced organizations to allocate scarce funds for system recovery rather than economic development.

3.**Cryptocurrency laundering**. Illicit financial flows through cryptocurrency platforms facilitate money laundering and fund militant activities, destabilizing economies. In Syria, illicit cryptocurrency mining has become a major source of funding for organized crime groups, undermining the nation's economic recovery.

The economic implications of cybercrime extend beyond immediate financial losses to include the erosion of trust in public and private institutions. This erosion has profound effects on national security and economic resilience.

1.**Impact on public institutions**. Cyberattacks targeting government databases and systems erode public confidence in the state's ability to protect sensitive information and maintain functional governance. For instance, phishing attacks during the

Nagorno-Karabakh conflict compromised government communications, weakening public trust in national leadership.

2.**Private sector vulnerabilities**. Repeated cyberattacks on businesses, including financial institutions, reduce consumer trust in digital platforms. This hesitancy hampers the adoption of digital technologies, slowing economic modernization and increasing transaction costs.

3.**Global perception**. Nations perceived as cyber-insecure face reputational damage, reducing their attractiveness as destinations for investment and trade partnerships. The economic impact of such reputational losses can linger long after the conflict has ended.

Cybercrime disproportionately affects weaker economies, exacerbating existing inequalities between nations. Developing countries often lack the technological infrastructure and human capital needed to counteract sophisticated cyber threats, making them attractive targets for cybercriminals.

1.**Regional disparities.** In Sub-Saharan Africa, limited cybersecurity capabilities have allowed organized crime groups to exploit financial systems with relative ease, deepening economic disparities between the region and more cyber-secure nations. The asymmetric impact of cybercrime creates a vicious cycle where vulnerable economies become further destabilized, reducing their capacity to invest in resilience.

2.**Humanitarian costs**. Cybercrime in wartime disrupts the delivery of humanitarian aid, compounding economic vulnerabilities. For example, fraudulent schemes targeting aid distribution in Yemen delayed the delivery of essential supplies, exacerbating the economic and human toll of the conflict.

Economic vulnerabilities caused by cybercrime have direct implications for national security, as weakened economies struggle to sustain military operations, rebuild infrastructure, and address societal needs.

1.**Reduced military capacity.** Financial losses from cybercrime limit a nation's ability to fund defense initiatives, purchase equipment, and train personnel. Prolonged economic strain can reduce a nation's ability to maintain a prolonged conflict, shifting the balance of power in favor of adversaries.

2.**Destabilization of governance**. Cybercrime that targets economic systems contributes to political instability by exacerbating unemployment, inflation, and public discontent. In Afghanistan, the diversion of funds through digital fraud weakened the government's legitimacy and its ability to counter insurgent groups.

3.**Global Security Risks**. Transnational cybercrime networks often exploit wartime economies to fund international terrorism, trafficking, and organized crime, creating security risks that transcend borders. This interconnectedness

underscores the need for coordinated international responses to combat cybercrime in conflict zones.

The role of cybercrime in exacerbating economic vulnerabilities during wartime cannot be overstated. By disrupting critical infrastructure, diverting financial resources, and undermining institutional trust, cybercrime compounds the challenges faced by nations in conflict. These economic repercussions, in turn, weaken national security, creating a feedback loop of instability that prolongs recovery and increases the risk of further conflict. Addressing these challenges requires a multifaceted approach that combines robust cybersecurity measures, international cooperation, and investments in resilience to safeguard both economic stability and national security in an increasingly interconnected world.

3.3 **Digital tools in combating cybercrime, financial fraud and corruption**[10]

The rise of blockchain and artificial intelligence (AI) technologies has transformed the fight against cybercrime and corruption, offering innovative solutions that enhance detection,

[10] This chapter was prepared as part of a research project 0124U000544

prevention, and accountability. Blockchain technology provides an immutable ledger system, making it a powerful tool for tracking financial transactions and identifying anomalies indicative of fraud or corruption. The integration of AI, with its ability to analyze vast datasets in real time, further strengthens these efforts.

1. **Applications in fraud detection**: blockchain systems ensure that financial transactions are tamper-proof, reducing the risk of manipulation. AI algorithms can identify irregularities in transactional patterns, flagging potential instances of fraud. Estonia's e-Residency program leverages blockchain for secure digital identity verification, reducing fraud in public services.

2. **Corruption monitoring**: AI-powered tools analyze procurement processes and governmental spending to identify red flags indicative of corrupt practices. Combined with blockchain, these tools ensure transparency by creating publicly accessible records of transactions. In Ukraine, ProZorro, an e-procurement system utilizing AI and blockchain, has significantly reduced corruption in public procurement.

3. **Transparency improvement**: Blockchain creates a transparent system where all stakeholders can access data, ensuring accountability. AI augments this by analyzing and presenting insights into data trends, enabling policymakers to make informed decisions.

Table 3.5 – Blockchain and AI Applications in Combating Cybercrime

Application	Key Features	Example
Fraud Detection	Identifying irregularities in transactions	Estonia's e-Residency Program
Corruption Monitoring	Flagging anomalies in procurement processes	Ukraine's ProZorro System
Transparency Improvement	Creating accessible, tamper-proof records	Publicly available blockchain audits

Digital tools integrated into governance systems have revolutionized the fight against corruption, providing efficient, transparent, and accountable frameworks.

1. **Integration of digital tools**: E-governance systems reduce bureaucratic inefficiencies and limit opportunities for corrupt practices by automating processes. Tools like digital tax systems, e-courts, and e-voting enhance transparency.

– **India**: the Aadhaar program, a digital identity system, has minimized corruption in welfare schemes by ensuring direct benefit transfers.

– **Georgia**: the introduction of e-governance platforms streamlined public services and eliminated intermediaries, reducing corruption opportunities.

2. **Impact on Governance**: The use of digital tools has increased public trust in government institutions by ensuring that processes are fair and transparent. Automated monitoring and

reporting mechanisms have made governance systems more resilient to cyber threats and corruption.

Countries facing wartime corruption and cybercrime have adopted comprehensive cybersecurity policies tailored to address these challenges. These policies emphasize prevention, detection, and response.

1. **Prevention strategies**:

– developing national cybersecurity frameworks that align with international standards;

– conducting awareness campaigns to educate citizens and organizations about cyber risks;

2. **Detection strategies**:

– establishing cybersecurity task forces to monitor digital threats in real time;

– collaborating with private sector entities to share intelligence and develop robust defenses.

3. **Response strategies**:

– implementing incident response protocols to mitigate damage during cyberattacks;

– investing in cyber resilience programs to ensure the continuity of critical operations.

Table 3.6 – Cybersecurity Strategies to Combat Wartime Corruption

Strategy	Description	Example
Prevention	Developing frameworks, educating citizens	National cybersecurity campaigns
Detection	Monitoring threats, sharing intelligence	Real-time cyber task forces
Response	Mitigating damage, ensuring resilience	Incident response protocols

3.4 Cybersecurity in shadow economies during wartime[11]

Wartime environments disrupt traditional economic and governance systems, creating a fertile ground for shadow economies to thrive. These economies, characterized by illicit and unregulated financial activities, exploit weakened institutions, lack of oversight, and the chaotic nature of conflict zones. Examples include smuggling, black markets, counterfeit operations, and illicit financial flows, which collectively undermine national security, economic recovery, and societal stability. The digital transformation of economic processes further complicates this issue, as cyber tools enable more sophisticated and less traceable criminal activities.

[11] This chapter was prepared as part of a research project 0124U000544

Cybersecurity is increasingly recognized as an indispensable tool in the fight against shadow economies during wartime. From tracking illicit financial flows to dismantling online marketplaces for counterfeit goods, advanced technologies such as blockchain, artificial intelligence (AI), and machine learning offer unprecedented opportunities to address the challenges posed by these covert economies. This section examines the role of cybersecurity in combating shadow economies, providing a detailed exploration of its applications, technological innovations, and policy implications.

The role of cybersecurity in wartime is amplified by the evolving nature of shadow economies. During conflicts, these economies often act as parallel systems to provide illicit goods and services, including weapons, human trafficking, counterfeit goods, and unregulated financial transfers. The digital infrastructure used by these economies – ranging from cryptocurrency networks to dark web marketplaces – poses a direct threat to state authority and governance. Cybersecurity tools serve as the primary mechanism to counter these threats by:

– **tracing illicit transactions**: monitoring financial flows through blockchain analytics to detect money laundering and fund transfers to criminal organizations;

– **identifying criminal networks**: analyzing communication patterns and digital footprints to uncover organized groups involved in shadow economic activities;

– **protecting critical infrastructure**: ensuring the resilience of financial, communication, and energy networks against cyberattacks initiated by shadow economy actors.

Technological applications in shadow economy monitoring:

1. **Blockchain technology**:

– enables real-time tracking of financial transactions;

– detects irregularities in cryptocurrency exchanges and peer-to-peer networks;

– example: monitoring funds allocated for humanitarian aid to prevent diversion into illicit markets.

2. **Artificial intelligence and machine learning**:

– analyzes large datasets to identify patterns associated with illicit activities;

– predicts vulnerabilities in digital systems that shadow economies might exploit.

3. **Dark web monitoring**:

– identifies platforms and marketplaces facilitating illegal transactions;

– tracks discussions and advertisements related to smuggling, counterfeit goods, and human trafficking.

Table 3.7 – Key cybersecurity tools for combating shadow economies

Technology	Application	Impact
Blockchain Analytics	Monitoring cryptocurrency transactions for anomalies.	Improved traceability of illicit financial flows.
Artificial Intelligence	Detecting patterns in financial activities and communication networks.	Enhanced detection of organized criminal groups.
Dark Web Scraping	Identifying illicit marketplaces and forums.	Reduction in the online facilitation of shadow economy activities.
Cryptographic Systems	Protecting sensitive governmental and financial data.	Secured information systems critical to economic stability.

A comprehensive policy framework integrating cybersecurity measures can effectively disrupt shadow economic activities. Such policies should include:

– mandatory reporting of cyber threats**:** establishing legal frameworks that require organizations to report cyber incidents and suspicious activities;

– public-private partnerships**:** encouraging collaboration between governmental agencies and private tech firms to develop innovative solutions for monitoring shadow economies;

– international collaboration**:** engaging with international organizations to harmonize cybersecurity protocols and share intelligence.

Regulatory challenges:

– ensuring compliance with cybersecurity protocols in regions with limited digital literacy;

– addressing jurisdictional issues in cross-border cybercrime investigations.

Table 3.8 – Policy recommendations for cybersecurity integration

Policy Recommendation	Objective	Expected Outcome
Enhanced Legal Frameworks	Regulating digital financial systems and cryptocurrencies.	Reduced exploitation of unregulated financial tools by shadow economies.
Cybersecurity Awareness Campaigns	Educating businesses and individuals on best practices.	Increased resilience against phishing and ransomware attacks.
International Agreements	Facilitating cross-border cybercrime investigations.	Improved global cooperation in combating transnational shadow economies.

Case studies of cybersecurity in action:

1. **Ukraine**:

– Context**:** post-2014 conflict zones saw a surge in cryptocurrency-based money laundering.

– Cybersecurity intervention**:** deployment of blockchain analytics to monitor illicit financial activities.

– Outcome**:** significant reduction in the misuse of digital financial systems for shadow economy activities.

2. **Syria**:

– Context**:** dark web marketplaces facilitated the sale of weapons and counterfeit goods.

– Cybersecurity intervention**:** collaborative international efforts to dismantle these platforms.

– Outcome**:** disruption of critical supply chains for shadow economy actors.

3. **Afghanistan**:

– Context**:** the use of counterfeit documentation to access reconstruction funds.

– Cybersecurity intervention**:** implementation of secure cryptographic systems for data verification.

– Outcome: enhanced transparency and reduced fraudulent claims.

Digital technologies provide a twofold advantage: they offer tools to suppress shadow economic activities while simultaneously building resilience in legitimate economic systems. Key applications include:

1.**Blockchain for aid distribution**: ensuring transparent allocation and tracking of international aid.

2.**AI-driven predictive models**: anticipating future vulnerabilities and devising proactive countermeasures.

3.**Cryptographic security**: securing government databases and preventing unauthorized access.

Table 3. 9 – Use of digital technologies in economic stabilization

Technology	Application	Impact
Blockchain	Tracking reconstruction funds.	Ensures transparency and minimizes corruption risks.
Artificial Intelligence	Predicting illicit financial activities.	Proactive identification and mitigation of risks.
Cryptographic Systems	Protecting sensitive data during post-war recovery.	Enhanced trust in governmental and financial institutions.

Shadow economies during wartime pose complex challenges to national security and post-conflict recovery. The integration of advanced cybersecurity measures is essential to disrupt these illicit networks and ensure economic stabilization. By leveraging blockchain, AI, and cryptographic systems, nations can effectively combat shadow economic activities while fostering transparency and resilience in legitimate economic processes. A coordinated approach involving policy reform, international cooperation, and technological innovation is imperative for sustainable recovery and the long-term suppression of shadow economies.

3.5 Post-War strategies for cybercrime prevention and economic recovery[12]

Military conflicts create a heightened risk of cyberattacks as adversaries target critical infrastructure, disrupt communication systems, and exploit the chaos of war to further their objectives. For Ukraine, addressing these threats requires proactive measures to safeguard both civilian and military digital ecosystems.

Key strategies:

1. **Real-time threat monitoring**:

– establish a centralized war-time cybersecurity command center to monitor and respond to cyber threats targeting critical infrastructure such as energy, healthcare, and transportation systems;

– leverage ai-driven systems for real-time threat detection and rapid response;

– develop protocols for incident reporting and immediate mitigation actions.

2. **Cybersecurity for military operations**:

[12] This chapter was prepared as part of a research project 0124U000544

– implement secure communication channels for military operations to prevent espionage and disruption;

– deploy encryption technologies to protect sensitive military data;

– regularly update and audit military cybersecurity practices to address emerging vulnerabilities.

3. **Public Awareness and Resilience**:

– launch national campaigns to educate the public and businesses about phishing, ransomware, and misinformation during wartime;

– provide resources and guidelines to strengthen individual and organizational cybersecurity practices.

4. **Collaboration with Allies**:

– foster international partnerships to share intelligence on emerging cyber threats;

– engage with NATO's Cooperative Cyber Defence Centre of Excellence for expertise and coordinated defense efforts.

Table 3.10 – War-time cybercrime prevention strategies

Focus Area	Key Actions	Expected Outcomes
Real-Time Threat Monitoring	Establishment of centralized command centers; use of AI for rapid detection.	Immediate identification and neutralization of threats.
Military Cybersecurity	Encryption and secure communication systems; regular audits.	Enhanced protection of military operations.
Public Awareness	Nationwide educational campaigns; resources for businesses and individuals.	Increased public resilience against cyber threats.
International Collaboration	Intelligence sharing; partnerships with global cybersecurity organizations.	Improved coordination and defense capabilities.

The aftermath of military conflicts presents unique challenges for economic recovery and the restoration of governance structures. Cybersecurity must be an integral component of post-war strategies, ensuring that digital infrastructure and financial systems remain secure from the persistent threats of cybercrime. Effective integration of cybersecurity into post-war economies involves targeted policy frameworks, technological investments, and capacity-building initiatives.

Key policy recommendations**:**

– Developing comprehensive cybersecurity frameworks**:** governments should establish robust cybersecurity policies tailored to the unique vulnerabilities of post-conflict environments. These frameworks must prioritize the protection

of critical infrastructure, including financial systems, energy grids, and communication networks (Table 3.11).

– Strengthening digital resilience**:** investments in modern technologies, such as blockchain for secure transactions and AI for threat detection, are critical. Resilient systems should include mechanisms for real-time monitoring and rapid response to cyber threats.

– Promoting public-private partnerships**:** collaboration between governmental agencies and private sector entities can enhance cybersecurity capabilities. Such partnerships facilitate knowledge sharing, resource pooling, and the adoption of best practices. Post-genocide, Rwanda integrated digital governance with cybersecurity frameworks, fostering economic growth while mitigating risks associated with cybercrime.

Table 3.11 – Cybersecurity integration into post-war economies

Focus Area	Key Actions	Expected Outcome
Critical Infrastructure	Secure energy grids, communication networks, and financial systems	Enhanced economic stability and reduced risks
Policy Development	Tailored cybersecurity frameworks focusing on conflict-related vulnerabilities	Resilient digital and financial ecosystems
Technology Investments	Integration of AI for threat detection and blockchain for secure transactions	Proactive threat detection and prevention

Public-Private Partnerships	Collaborative resource pooling, coordinated cyber defense strategies	Effective knowledge sharing and innovation

Table 3.11 highlights the multifaceted approach required to integrate cybersecurity into post-war economies. By addressing critical infrastructure, policy development, technology investments, and partnerships, nations can build resilient systems capable of mitigating cyber threats.

Combatting organized cybercrime in the post-war period requires long-term strategies that address the transnational nature of these threats. Organized cybercriminal groups often exploit jurisdictional gaps and weak international collaboration to perpetrate their schemes.

Mechanisms for cross-border collaboration**:**

– International intelligence sharing**:** countries must establish secure channels for exchanging intelligence on cyber threats. Real-time sharing of information enables preemptive action against organized cybercrime networks (Table 3.12);

– standardization of cybersecurity protocols: harmonizing cybersecurity laws and protocols across countries facilitates cooperative enforcement actions and reduces operational barriers in countering cyber threats;

– capacity building in emerging economies**:** assisting post-conflict nations in building cybersecurity capabilities ensures that global cyber defense networks are uniformly robust.

Example**:** the European Union's Network and Information Security (NIS) Directive serves as a model for fostering collaboration among member states, enhancing collective cyber resilience.

Table 3.12 – Key elements for cross-border cybercrime collaboration

Element	**Description**	**Examples of Implementation**
Regional Cybersecurity Centers	Act as hubs for threat analysis, coordinated response, and training.	European Union's NIS Directive
Standardized Protocols	Harmonized legal and technical standards to facilitate international cooperation.	Interpol's Global Cybercrime Program
Training and Capacity Building	Professional development programs for cybersecurity experts in emerging economies.	Cybersecurity workshops led by NATO
Real-Time Intelligence Sharing	Systems for instant sharing of actionable data on cyber threats across borders.	ASEAN's Cybersecurity Cooperation Framework

Table 3.12 underscores the importance of structured collaboration mechanisms to combat transnational cybercrime. By standardizing protocols and enhancing intelligence sharing, nations can collectively address these pervasive threats while fostering global cybersecurity resilience.

To address the challenges of cybercrime during and after military conflict, Ukraine must implement a comprehensive and phased approach. Below is a detailed roadmap outlining the necessary steps to enhance cybersecurity and facilitate economic recovery.

Table 3.13 – War and post-war cybercrime prevention roadmap

Phase	Key Actions	Expected Outcomes
Phase 1: Immediate (During War)	Conduct real-time monitoring of cyber threats targeting critical infrastructure. Establish rapid-response cybersecurity teams.	Immediate mitigation of cyber threats and stabilization of essential services.
Phase 2: Immediate (During War)	Enhance public awareness campaigns on phishing and ransomware threats tailored for wartime conditions.	Increased public resilience to common cybercrime tactics.
Phase 3: Short-Term (Post-War)	Develop and enforce national cybersecurity legislation emphasizing wartime lessons. Create a centralized database for reporting cyber incidents.	Strengthened legal framework and better coordination of cybersecurity responses.
Phase 4: Medium-	Establish regional cybersecurity hubs to share	Improved regional collaboration and

Term (Post-War)	intelligence and coordinate responses across administrative regions.	preparedness for complex cyber threats.
Phase 5: Medium-Term (Post-War)	Deploy blockchain technologies for secure transaction monitoring, especially for reconstruction funds and aid programs.	Enhanced transparency and reduced fraud in post-war economic activities.
Phase 6: Long-Term (Post-War)	Launch capacity-building programs for cybersecurity professionals, focusing on advanced techniques like AI-driven threat analysis.	Sustainable development of national cybersecurity expertise.
Phase 7: Long-Term (Post-War)	Pursue international cooperation for cyber intelligence sharing and harmonization of cybersecurity standards.	Better coordination with international partners and strengthened defenses.
Phase 8: Long-Term (Post-War)	Invest in cutting-edge technologies such as quantum cryptography and adaptive cybersecurity solutions to counter advanced threats.	Proactive adaptation to emerging threats and long-term digital resilience.

Phase 1 & 2: Immediate (During War):

– real-time monitoring: Ukraine's critical infrastructure, including energy grids, healthcare systems, and financial institutions, faces heightened risks during conflict. Implementing 24/7 monitoring systems and deploying incident response teams ensures rapid mitigation of cyber threats;

– public awareness campaigns: tailored educational campaigns focusing on phishing, ransomware, and

misinformation help reduce the susceptibility of individuals and organizations to cyberattacks.

Phase 3: Short-Term (Post-War):

– legislative frameworks: wartime experiences must inform robust cybersecurity legislation. This includes establishing clear accountability mechanisms for cyber incidents and penalties for breaches.

– centralized reporting database: a unified platform for reporting and analyzing cyber incidents allows for trend identification and enhances response capabilities.

Phase 4 & 5: Medium-Term (Post-War):

– regional cybersecurity hubs: decentralizing cybersecurity operations through regional hubs ensures swift response capabilities tailored to local contexts. These hubs can also serve as training centers;

– blockchain Implementation: leveraging blockchain technology for reconstruction efforts minimizes corruption and ensures the secure distribution of financial resources and aid.

Phase 6-8: Long-Term (Post-War):

– capacity building: developing advanced training programs for cybersecurity experts strengthens national defenses. collaboration with academic institutions and private entities is key;

– international cooperation: active participation in global cybersecurity initiatives facilitates knowledge sharing and collective action against transnational cyber threats.

– investment in advanced technologies: quantum cryptography and adaptive AI solutions offer forward-looking protection against sophisticated cyberattacks. These investments future-proof national infrastructure.

This roadmap provides a structured approach to addressing cybercrime during and after military conflict. By focusing on immediate actions, medium-term stabilization, and long-term resilience, Ukraine can strengthen its digital defenses and support economic recovery. The integration of advanced technologies and international collaboration will ensure sustained security and prosperity in the post-war period.

Conclusions to Chapter 3

Chapter 3 synthesized extensive research and analysis on the transformative role of cybersecurity and digital tools in combating wartime and post-war challenges, including cybercrime, financial fraud, corruption, and the shadow economy. It provided a detailed examination of the multifaceted threats posed by cybercriminals and how digital transformation can serve as both a vulnerability and a solution. The insights

drawn from this chapter underscore critical lessons for governments, policymakers, and international organizations.

The analysis demonstrated that wartime conditions exacerbate the risks of cybercrime, with attacks targeting critical infrastructure, financial systems, and social stability. These threats disrupt not only immediate operations but also the broader economic and institutional frameworks necessary for recovery. Countries engaged in military conflict, such as Ukraine, Syria, and Afghanistan, provided illustrative examples of how cybercrime evolves during conflict, exploiting weakened governance, societal vulnerabilities, and the rapid adoption of digital technologies.

One of the chapter's central findings was the significant role of digital tools in addressing these challenges. Blockchain emerged as a pivotal technology for ensuring transparency in financial transactions and mitigating fraud in reconstruction efforts. Artificial intelligence and machine learning were highlighted for their ability to detect and predict cyber threats, analyze large-scale data for patterns of corruption, and enhance overall system resilience. The integration of these tools into e-governance frameworks was shown to be instrumental in reducing corruption and increasing accountability during both wartime and post-war recovery.

The chapter also revealed the critical interplay between shadow economies and cybersecurity. Wartime shadow economies, often fueled by cybercrime, create a parallel system that undermines legitimate economic activities and governance. Digital tools, such as dark web monitoring and data analytics, were shown to be effective in identifying and disrupting these illicit networks. However, these tools require robust institutional capacity and international cooperation to achieve their full potential.

In exploring post-war strategies, the chapter emphasized the importance of integrating cybersecurity into broader economic recovery plans. A phased approach was recommended, beginning with immediate measures to secure critical infrastructure and progressing toward long-term investments in advanced technologies, capacity-building, and international collaboration. The findings also highlighted the necessity of aligning these efforts with global cybersecurity standards to address transnational threats and foster collective resilience.

The overarching conclusion of this chapter is that the integration of cybersecurity and digital tools is not just a response to cyber threats but a foundational component of modern governance and economic stability. While the digital transformation of wartime and post-war economies introduces

new risks, it also provides unprecedented opportunities to address these challenges with precision and efficiency. Policymakers and stakeholders must adopt a holistic approach that combines technological innovation, strategic policymaking, and international collaboration to build resilient societies capable of withstanding the multifaceted threats of the cyber age.

By leveraging the insights from this chapter, governments and institutions can move beyond reactive measures to implement proactive and sustainable strategies. These efforts are essential for safeguarding economic recovery, ensuring social trust, and maintaining national security in an increasingly digital and interconnected world.

CONCLUSIONS

This monograph provides an in-depth exploration of financial fraud, money laundering, corruption, shadow economies, and cybercrime in the context of wartime and post-war recovery, yielding significant insights and practical implications. Across three chapters, the research examines the mechanisms, systemic implications, and evolving strategies needed to address these pervasive issues effectively.

The analysis in the Chapter 1 revealed that financial fraud, money laundering, and corruption are deeply interwoven with the socio-economic dynamics of conflict-affected regions. The findings emphasized how weakened governance structures and economic dislocation create fertile ground for these crimes to thrive. Shadow economies emerge as survival mechanisms but also exacerbate systemic inequalities and weaken formal economic systems. The research demonstrated the critical role of governance frameworks, transparency measures, and technological tools in mitigating these challenges. By employing bibliometric analysis, this chapter highlighted global research efforts, identifying key thematic clusters and regional contributions, underscoring the importance of international collaboration in addressing financial crimes.

The Chapter 2 advanced the understanding of cybersecurity and organized cybercrime in wartime, emphasizing the dynamic and transnational nature of these threats. The typologies of cybercrime, including ransomware attacks, phishing schemes, and state-sponsored cyber operations, were critically examined, revealing their profound impact on critical infrastructure and national security. The clustering of academic achievements illuminated the interdisciplinary nature of cybersecurity research and its evolving focus on adaptive strategies and technological innovation. The findings highlighted the urgent need for robust international cooperation, advanced technological solutions, and flexible policy frameworks to combat cybercrime effectively in conflict zones.

In the Chapter 3, the transformative potential of digital tools in combating financial crimes and cyber threats was explored in detail. Blockchain, artificial intelligence, and e-governance frameworks emerged as key instruments in enhancing transparency, detecting anomalies, and ensuring accountability in managing financial systems. The study also emphasized the critical role of integrating these tools into post-war recovery plans, which must prioritize capacity building, sustainability, and inclusivity. The analysis demonstrated how shadow economies disrupt recovery efforts and proposed

targeted interventions to dismantle these networks. Furthermore, long-term strategies for resilience, including the adoption of green transitions and public-private collaborations, were presented as essential components of sustainable recovery.

The research across these chapters reveals the systemic and interconnected nature of financial and cybercrimes in wartime, highlighting the global implications of these challenges. The findings underscore the need for comprehensive and integrated approaches that align governance reforms, technological innovations, and international cooperation. By addressing the root causes and leveraging advanced tools, it is possible to mitigate the socio-economic impacts of these crimes and foster resilient recovery.

Future research should focus on regional dynamics, the scalability of innovative solutions, and the integration of green and digital transitions in post-conflict recovery strategies. This monograph provides a robust framework for policymakers, practitioners, and academics to develop actionable strategies for addressing financial fraud, cybercrime, and related phenomena in an increasingly digital and interconnected world.

.

REFERENCES

1. ACAPS ANALYSIS HUB. (2024). Afghanistan: Mapping informal economies in informal settlements as a local integration pathway for IDPs (Thematic report). ACAPS.
2. Adebanwi, W., & Obadare, E. (2011). When corruption fights back: Democracy and elite interest in Nigeria's anti-corruption war. *Journal of Modern African Studies, 49*(2), 185–213. https://doi.org/10.1017/S0022278X11000012
3. Alexander, D. (2015). Disaster and Emergency Planning for Preparedness, Response, and Recovery. In *Oxford Research Encyclopedia of Natural Hazard Science*. Oxford University Press. https://doi.org/10.1093/acrefore/9780199389407.013.12
4. Antonio, J. M. A. (2024). Disparities and backlogs in Mexico's national and international cybersecurity policies vis-à-vis the United States and Canada: Challenges of cooperation for North America. *Norteamerica, 19*(1). https://doi.org/10.22201/cisan.24487228e.2024.1.663
5. Anvik, J., Cote, V., & Riehl, J. (2019). Program wars: A card game for learning programming and cybersecurity concepts. *SIGCSE 2019 - Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 393–399. https://doi.org/10.1145/3287324.3287496
6. Arcuri, G., & Lu, S. (2022). Taiwan's Semiconductor Dominance: Implications for Cross-Strait Relations and the Prospect of Forceful Unification. CSIS. https://www.csis.org/blogs/perspectives-innovation/taiwans-semiconductor-dominance-implications-cross-strait-relations
7. Asare, K., Samusevych, Y. (2023). Exploring Financial Fraud, Tax Tools, and Economic Security Research: Comprehensive Bibliometric Analysis. *Financial Markets,*

Institutions and Risks, *7*(3), 136-146. https://doi.org/10.61093/fmir.7(3).136-146.2023

8. Bäck, H., Teorell, J., & Lindberg, S. I. (2019). Cabinets, prime ministers, and corruption: A comparative analysis of parliamentary governments in post-war Europe. *Political Studies*, *67*(1), 149–170. https://doi.org/10.1177/0032321718760806
9. Balas, A. N., & Kaya, H. D. (2024). Do Retailers Compete Against Informal Firms? A Comparison of the Periods of the Global Crisis and Post-Crisis. *SocioEconomic Challenges*, *8*(2), 215-233. https://doi.org/10.61093/sec.8(2).215-233.2024
10. Banna, H., Alam, A., Chen, X. H., & Alam, A. W. (2023). Energy security and economic stability: The role of inflation and war. *Energy Economics*, *126*, 106949. https://doi.org/10.1016/j.eneco.2023.106949
11. Barannyk, L., Dobrovolska, O., Taranenko, V., Koriahina, T. & Rybalchenko, L. (2021). Personal income tax as a tool for implementing state social policy. *Investment Management and Financial Innovations*, *18*(2), 287-297. doi:10.21511/imfi.18(2).2021.23
12. Bijańska,J.,Kuzior,A. & Wodarski,K.(2018).Social Perception of Hard Coal Mining in Perspective of Region's Sustainable Development. Management Systems in Production Engineering,26(3) 178-183. https://doi.org/10.1515/mspe-2018-0029
13. Bilan, Y., Srovnalã-KovÃi, P., Streimikis, J., Lyeonov, S., Tiutiunyk, I., & Humenna, Y. (2020b). From shadow economy to lower carbon intensity: Theory and evidence. International Journal of Global Environmental Issues, 19(1-3), 196-216. Retrieved from http://www.inderscience.com/ijgenvi
14. Bilan, Y., Tiutiunyk, I., Lyeonov, S., & Vasylieva, T. (2020a). Shadow economy and economic development: A

panel cointegration and causality analysis. International Journal of Economic Policy in Emerging Economies, 13(2), 173-193. doi:10.1504/IJEPEE.2020.107929
15. Bo Jensen, S., & Hapal, K. (2018). Police violence and corruption in the Philippines: Violent exchange and the war on drugs. *Journal of Current Southeast Asian Affairs, 37*(2), 39–62. https://doi.org/10.1177/186810341803700202
16. Bouyacoub, B. (2024). Empirical Exploration of Economic Policy in the Middle East and North Africa (MENA) Region: An ARDL Approach. *Financial Markets, Institutions and Risks, 8*(1), 158-172. https://doi.org/10.61093/fmir.8(1).158-172.2024
17. Bygrave, L. A. (2025). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. *Computer Law and Security Review, 56,* 106071. 10.1016/j.clsr.2024.106071
18. Cercel, C. (2024). Darker legacies of anti-corruption: Fascist criticisms of the law in inter-war Romania. *International Journal of Law in Context.* https://doi.org/10.1177/0022343308100715
19. Chung, D. (2024). The Cold War history of wheat flour in South Korea, 1945–1960: The discourse of corruption and the April Revolution of 1960. *Cold War History.* https://doi.org/10.1080/14682745.2024.2341225
20. Cifuentes-Faura, J. (2024). Corruption in Ukraine during the Ukrainian–Russian war: A decalogue of policies to combat it. *Journal of Public Affairs, 24*(1), e2905. https://doi.org/10.1002/pa.2905
21. Collier, P., & Hoeffler, A. (2004). Greed and Grievance in Civil War. *Oxford Economic Papers, 56*(4), 563–595.
22. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007
23. Didenko, I., Petrenko, K. & Pudlo, T. (2023). The role of financial literacy in ensuring financial inclusion of the

population. *Financial Markets, Institutions and Risks, 7*(2), 72-79. https://doi.org/10.21272/fmir.7(2).72-79.2023
24. Djouadi, I., Zakane, A., & Abdellaoui, O. (2024). Corruption and Economic Growth Nexus: Empirical Evidence From Dynamic Threshold Panel Data. *Business Ethics and Leadership, 8*(2), 49-62. https://doi.org/10.61093/bel.8(2).49-62.2024
25. Dluhopolskyi, O., & Danyliuk, I. (2023). ECONOMIC EVALUATION OF THE ELECTRONIC PUBLIC PROCUREMENT SYSTEM: THE CASE OF PROZORRO 2018-2022. *Socio-Economic Relations in the Digital Society*, *4*(50), 95-111. https://doi.org/10.55643/ser.4.50.2023.517
26. Dobrovolska, O., Sonntag, R., Mynenko, S., & Kosyk, D. (2024a). A Fair Investment Environment: The Impact of the Shadow Economy, the Harshness of the Courts Against Corrupt Officials, Tax Pressure and Restrictions on Business. *Business Ethics and Leadership, 8*(2), 200-218. https://doi.org/10.61093/bel.8(2).200-218.2024
27. Dobrovolska, O., Sonntag, R., Kachula, S., Lysiak, L. & Lastovchenko, P. (2024b). Tax policy and activation of internal factors of economic growth: EU experience for Ukraine. *Public and Municipal Finance*, *13*(1), 70-82. doi:10.21511/pmf.13(1).2024.06
28. Doig, A., & Tisne, M. (2009). A candidate for relegation? Corruption, governance approaches and the (re)construction of post-war states. *Public Administration and Development, 29*(5), 374–386. https://doi.org/10.1002/pad.543
29. Fearon, J., & Laitin, D. (2003). Ethnicity, Insurgency, and Civil War. *American Political Science Review, 97*(01), 75–90. https://doi.org/10.1017/S0003055403000534
30. Filatova, H., Voytov, S., Polishchuk, Y. & Dudchyk, O. (2022). The public debt of Ukraine in the economic development policy in the war and post-war periods: Bibliometric analysis. *Public and Municipal Finance*, *11*(1), 142-154. doi:10.21511/pmf.11(1).2022.12

31. Filemon, T., Lubbe, S., & Mynhardt, H. (2024). The Assessment of Risk Management in Human Resources Practices in the Public Sector. *SocioEconomic Challenges, 8*(2), 342-359. https://doi.org/10.61093/sec.8(2).342-359.2024
32. Fjelde, H. (2009). Buying peace? Oil wealth, corruption, and civil war, 1985-99. *Journal of Peace Research, 46*(2), 199–218. https://doi.org/10.xxxx/yyyy
33. Garlepow, L., Funke, N., & Güldenring, B. A. (2024). A multifactorial approach to war and corruption metaphors in South Asian Englishes. *World Englishes.* https://doi.org/10.1111/weng.12703
34. Gerd Junne, & Willemijn Verkoren. (2005). Postconflict development: Meeting new challenges. Lynne Rienner Publishers.
35. Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: War-fighting and national cybersecurity. *Journal of Homeland Security and Emergency Management, 7*(1), 22. https://doi.org/10.2202/1547-7355.1636
36. Hough, T., & Gross, K. A. (2019). Cybersecurity: Cyberspace wars-the unseen enemy. In *Advanced Practice and Leadership in Radiology Nursing* (pp. 285–289). https://doi.org/10.1007/978-3-030-32679-1_26
37. Kano, L., Narula, R., & Surdu, I. (2022). Global Value Chain Resilience: Understanding the Impact of Managerial Governance Adaptations. *California Management Review, 64*(2), 24–45. https://doi.org/10.1177/00081256211066635
38. Kaya, H.D. (2023). The global crisis, government contracts, licensing and corruption. *SocioEconomic Challenges, 7*(4), 1-7. https://doi.org/10.61093/sec.7(4).1-7.2023
39. Kelemen, R. (2023). The impact of the Russian-Ukrainian hybrid war on the European Union's cybersecurity policies and regulations. *Connections, 22*(2), 75–90. https://doi.org/10.11610/Connections.22.2.55

40. King, S., & Chaudry, K. (2022). *Losing the cybersecurity war: And what we can do to stop it.* (pp. 1–148). https://doi.org/10.1201/9781003331773
41. Kovbasyuk, L., Vakulenko, Y., Ivanets, I., Bozhenko, V., & Kharchenko, D. (2024). Forecast of Corruption: From Ethical to Pragmatic Considerations. *Business Ethics and Leadership*, *8*(2), 184-199. https://doi.org/10.61093/bel.8(2).184-199.2024
42. Kozhushko, I. (2023). Transformation of Financial Services Industry in Conditions of Digitalization of Economy. *Financial Markets, Institutions and Risks*, *7*(4), 189-200. https://doi.org/10.61093/fmir.7(4).189-200.2023
43. Kuzior A, Ober J, Karwot J. (2021). Stakeholder Expectation of Corporate Social Responsibility Practices: A Case Study of PWiK Rybnik, Poland. *Energies*. 14(11):3337. https://doi.org/10.3390/en14113337
44. Kuzior, A.; Arefieva, O.; Kovalchuk, A.; Brożek, P. & Tytykalo, V., (2022). Strategic Guidelines for the Intellectualization of Human Capital in the Context of Innovative Transformation. Sustainability, 14, 11937. DOI: 0.3390/su141911937
45. Kuzmenko, O., Bilan, Y., Bondarenko, E., Gavurova, B., & Yarovenko, H. (2023b). Dynamic stability of the financial monitoring system: Intellectual analysis. PLoS ONE, 18(1 January) doi:10.1371/journal.pone.0276533
46. Kuzmenko, O., Yarovenko, H. & Perkhun L. (2023a). Assessing the maturity of the current global system for combating financial and cyber fraud. Statistics in Transition new series, vol. 24, 1, 229-258 Published online: 24 February 2023https://doi.org/10.59170/stattrans-2023-013
47. Le Billon, P. (2003). Buying peace or fueling war: The role of corruption in armed conflicts. *Journal of International Development*, *15*(4), 413–426. https://doi.org/10.1002/jid.993

48. Le Billon, P. (2014). Natural resources and corruption in post-war transitions: Matters of trust. *Third World Quarterly*, *35*(5), 770–786. https://doi.org/10.1080/01436597.2014.921429
49. Lennerfors, T. T. (2007). The transformation of transparency: On the act on public procurement and the right to appeal in the context of the war on corruption. *Journal of Business Ethics*, *73*(4), 381–390. https://doi.org/10.1007/s10551-006-9213-3
50. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. Paper presented at the CEUR Workshop Proceedings, , 2422 297-307. Retrieved from https://www.scopus.com/record/display.uri?eid=2-s2.0-85071081226&origin=resultslist
51. Lesschaeve, C., & Glaurdić, J. (2022). Condoning postwar corruption: How legacies of war prevent democratic accountability in contemporary Southeast Europe. *East European Politics*, *38*(2), 188–207. https://doi.org/10.1080/21599165.2021.1965577
52. Lewis, J. (2021). Shaping the ground for bilateral cybersecurity negotiations. *China International Strategy Review*, *3*(1), 115–122. https://doi.org/10.1007/s42533-021-00081-z
53. Lindberg, J., & Orjuela, C. (2011). Corruption and conflict: Connections and consequences in war-torn Sri Lanka. *Conflict, Security and Development*, *11*(2), 205–233. https://doi.org/10.1080/14678802.2011.572455
54. Lindberg, J., & Orjuela, C. (2014). Corruption in the aftermath of war: An introduction. *Third World Quarterly*, *35*(5), 723–736. https://doi.org/10.1080/01436597.2014.921421
55. Maher, A. (2024). Tracing the bounds of distress: Mental health and the Lancet Commission on lessons for the future

from the COVID-19 pandemic. *Journal of Global Health, 14*. https://doi.org/10.7189/jogh.14.03022

56. Mańka-Szulik, M., Koibichuk, V., & Mogilina, A. (2024). Economic Determinants of Smart and Sustainable Urban Development: What Answers Does the Cities in Motion Index Give?. *SocioEconomic Challenges, 8*(2), 170-196. https://doi.org/10.61093/sec.8(2).170-196.2024
57. Maringira, G. (2017). Military corruption in war: Stealing and connivance among Zimbabwean foot soldiers in the Democratic Republic of Congo (1998–2002). *Review of African Political Economy, 44*(154), 611–623. https://doi.org/10.1080/03056244.2017.1406844
58. Martin, W. G. (2018). Lessons of the Northern War on African corruption. *Journal of Contemporary African Studies, 36*(4), 437–448. https://doi.org/10.1080/02589001.2018.1513125
59. Mazurenko, O., Tiutiunyk,I., Grytsyshen, D., Daňo, F., Artyukhov, A. & Rehak., R. (2023a). Good governance: Role in the coherence of tax competition and shadow economy. *Problems and Perspectives in Management*, *21*(4), 757-770. doi:10.21511/ppm.21(4).2023.56
60. Mazurenko, O., Tiutiunyk,I., Cherba, V., Artyukhov., A. & Yehorova, Y. (2023b). Shadow tax evasion and its impact on the competitiveness of the country's tax system. *Public and Municipal Finance*, *12*(2), 129-142. doi:10.21511/pmf.12(2).2023.11
61. Midor,K.,Kuzior,A.,Płaza,G.,Molenda,M. & Krawczyk,D.(2021).Reception of the Smart City Concept in the Opinion of Local Administration Officials – A Case Study. Management Systems in Production Engineering,29(4) 320-326. https://doi.org/10.2478/mspe-2021-0040
62. Miholic, J. (2023). The Hochenegg Affair in 1924: A facet of medical corruption in post-World War I Vienna | Die Hochenegg-Affäre 1924: Eine Facette medizinischer

Korruption im Nachkriegs-Wien der zwanziger Jahre. *Medizinhistorisches Journal*, *58*(4), 294–312. https://doi.org/10.25162/mhj-2023-0011

63. Mizrak, K. C. (2024). Crisis Management and Risk Mitigation. *Advances in Business Strategy and Competitive Advantage Book Series*, 254–278. https://doi.org/10.4018/979-8-3693-1155-4.ch013
64. Morin, S. L., & Burrell, D. N. (2024). Diversity Dishonesty: Smoke and Mirrors in the Organization. *SocioEconomic Challenges*, *8*(2), 109-125. https://doi.org/10.61093/sec.8(2).109-125.2024
65. Neudorfer, N. S., & Theuerkauf, U. G. (2014). Buying war not peace: The influence of corruption on the risk of ethnic war. *Comparative Political Studies, 47*(13), 1856–1886. https://doi.org/10.1177/0010414013516919
66. Nimko, O., Ohorodnyk, V., Dankevych, V., & Doronina, I. (2024). E-governance and corruption perception: Global insights and Ukraine's context during war and displacement. *Pakistan Journal of Criminology, 16*(3), 223–244. https://doi.org/10.62271/pjc.16.3.223.244
67. Normatovich, B. B., & Og'li Boboyorov, S. B. (2021). Cybersecurity and information war. *International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021*. https://doi.org/10.1109/ICISCT52966.2021.9670367
68. Nwozor, A., Olanrewaju, J. S., Oshewolo, S., & Ake, M. B. (2020). Is Nigeria really fighting to win the anti-corruption war? Presidential body language, "string-puppetting," and selective prosecutions. *Journal of Financial Crime, 27*(2), 601–617. https://doi.org/10.1108/JFC-08-2019-0109
69. Omotayo Bolodeoku, I. (2009). The war against corruption in Nigeria: A new role for the FIRS? *Journal of Money*

Laundering Control, *12*(4), 417–431. https://doi.org/10.1108/13685200910996092

70. Orjuela, C., Herath, D., & Lindberg, J. (2016). Corrupt peace? Corruption and ethnic divides in post-war Sri Lanka. *Journal of South Asian Development, 11*(2), 149–174. https://doi.org/10.1177/0973174116648818
71. Ostrom, E. (2010). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *American Economic Review*, *100*(3), 641–672.
72. Ozden, K., & Onapajo, H. (2019). Fighting the scourge from abroad: Anti-corruption war in Nigeria's foreign policy under the Buhari administration, 2015 to 2019. *African Renaissance, 16*(4), 157–175. https://doi.org/10.31920/2516-5305/2019/16N4A8
73. Park, D.-W., & Lee, S.-H. (2020). Hyperledger blockchain design for sharing, spreading, and protecting national cybersecurity information. *Journal of Information and Communication Convergence Engineering, 18*(2), 94–99. https://doi.org/10.6109/jicce.2020.18.2.94
74. Park, S., Kim, I. H., Kim, J., & Lee, K. L. (2018). The diagnosis and prescription for cybersecurity in Korea: Focusing on policy and system. *KSII Transactions on Internet and Information Systems, 12*(2), 843–859. https://doi.org/10.3837/tiis.2018.02.018
75. Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233–254. https://doi.org/10.1017/eis.2020.6
76. Posadnieva, O., & Sidelnykova, L. (2024). Fiscal and psychological factors of tax evasion. *Socio-Economic Relations in the Digital Society, 1*(51), 97-107. https://doi.org/10.55643/ser.1.51.2024.549
77. Ray, A. (2024). Gender, Race and Sectoral Inequality in Megacities: Case Study of Banking and Financial Services Industry. *Business Ethics and Leadership, 8*(2), 219-229. https://doi.org/10.61093/bel.8(2).219-229.2024

78. Samers, M. (2005). The Myopia of "Diverse Economies," or a Critique of the "Informal Economy." *Antipode, 37*(5), 875–886. https://doi.org/10.1111/j.0066-4812.2005.00537.x
79. Sheliemina, N. (2023). Analysis of implementing the Ukrainian healthcare reform in 2023. *Health Economics and Management Review*, *4*(4), 80-94. https://doi.org/10.61093/hem.2023.4-07
80. Slupska, J. (2021). War, health and ecosystem: Generative metaphors in cybersecurity governance. *Philosophy and Technology*, *34*(3), 463–482. https://doi.org/10.1007/s13347-020-00397-5
81. Springs, D. (2024a). Smart city planning focused on the US cities in need of policing innovations and public health safety technologies and strategies. *Health Economics and Management Review*, *5*(1), 117-128. https://doi.org/10.61093/hem.2024.1-09
82. Springs, D. (2024b). Elements of Smart Leadership Approaches for Smart City Development. *Business Ethics and Leadership*, *8*(2), 35-48. https://doi.org/10.61093/bel.8(2).35-48.2024
83. Steffen, B., & Patt, A. (2022). A historical turning point? Early evidence on how the Russia-Ukraine war changes public support for clean energy policies. *Energy Research & Social Science*, *91*, 102758. https://doi.org/10.1016/j.erss.2022.002758
84. Tareque, M. H., Deutekom, S., Anvik, J., & Bashir, M. (2024). You hacked my program! Teaching cybersecurity using game-based learning. *ACM International Conference Proceeding Series*, 8. https://doi.org/10.1145/3660650.3660672
85. Terepyshchyi, S., & Kostenko, A. (2022). Mapping the landscapes of cybersecurity education during the war in Ukraine 2022 | Mapowanie krajobrazów edukacji w zakresie cyberbezpieczeństwa podczas wojny na Ukrainie

2022. *Studia Warminskie, 59,* 125–135. https://doi.org/10.31648/SW.8331

86. Tromme, M., & Lara Otaola, M. A. (2014). Enrique Peña Nieto's national anti-corruption commission and the challenges of waging war against corruption in Mexico. *Mexican Studies - Estudios Mexicanos, 30*(2), 557–588. https://doi.org/10.1525/msem.2014.30.2.557
87. Uberti, L. J. (2014). Is separation of powers a remedy for the resource curse? Firm licensing, corruption and mining development in post-war Kosovo. *New Political Economy, 19*(5), 695–722. https://doi.org/10.1080/13563467.2013.849671
88. UNESCO. (2023, April 20). Education: From disruption to recovery. UNESCO. https://www.unesco.org/en/covid-19/education-disruption-recovery
89. UNHCR. (2022). Global Trends Report 2022. UNHCR. https://www.unhcr.org/global-trends-report-2022
90. Vasylieva, T. A., Kasyanenko, V. O., 2013. Integral assessment of innovation potential of ukraine's national economy: A scientific methodical approach and practical calculations. Actual Problems of Economics, 144(6), 50-59. Retrieved from https://www.scopus.com/record/display.uri?eid=2-s2.0-84923539973&origin=resultslist
91. Vilpišauskas, R. (2024). Gradually and then suddenly: The effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania. *Policy Studies, 45*(3-4), 467–488. https://doi.org/10.1080/01442872.2024.2311155
92. Wang, C. (2017). The dark side of the war: Corruption in the Guomindang government during World War II. *Journal of Modern Chinese History, 11*(2), 249–263. https://doi.org/10.1080/17535654.2017.1391006
93. Wedeman, A. (2008). Win, lose, or draw? China's quarter-century war on corruption. *Crime, Law and Social Change, 49*(1), 7–26. https://doi.org/10.1007/s10611-007-9088-y

94. World Bank, & UNICEF. (2022). The State of Global Learning Poverty.
95. Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, *4*(4), 17-27. https://doi.org/10.61093/hem.2023.4-02
96. Yergin, D. (2023, October 16). The 1973 Oil Crisis: Three Crises in One—and the Lessons for Today. *Center on Global Energy Policy at Columbia University SIPA.* https://www.energypolicy.columbia.edu/publications/the-1973-oil-crisis-three-crises-in-one-and-the-lessons-for-today/
97. Zámek, D., Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. *Financial Markets, Institutions and Risks*, *8*(1), 173-188. https://doi.org/10.61093/fmir.8(1).173-188.2024

FINANCIAL FRAUD AND CYBERCRIME IN WARTIME: AN OVERVIEW OF THE SCIENTIFIC LANDSCAPE AND INSIGHTS FROM COUNTRIES ENGAGED IN MILITARY CONFLICT

Dr Prof Serhiy LYEONOV
Dr Prof Tetiana VASYLIEVA
Ph.D. Hanna FILATOVA

Abstract

Addressing the critical challenges of financial fraud, money laundering, corruption, shadow economies, and cybercrime during wartime and post-war recovery, this monograph explores how these systemic issues exploit vulnerabilities exacerbated by conflict. It highlights how weakened governance, disrupted economies, and the rapid evolution of cyber threats create an environment where such crimes thrive, undermining recovery efforts and societal stability. Using advanced analytical techniques and case studies, the study provides a comprehensive examination of these interconnected phenomena and their implications for security, governance, and resilience.

The research identifies key patterns through the typologization of financial fraud and cybercrime schemes, emphasizing how these activities adapt to the chaos of war and transition into post-conflict periods. Shadow economies are revealed as both survival mechanisms and destabilizing forces, weakening formal economic structures and fostering organized criminal networks. In addition, the study conducts clustering and bibliometric analysis of scientific research, uncovering dominant thematic clusters and mapping global research efforts. This analysis highlights significant contributions from international academic networks and provides insights into evolving research priorities, particularly in integrating technology to combat these crimes.One of the study's major contributions is the development of a roadmap for post-war recovery and crime prevention strategies. This roadmap outlines immediate, medium-term, and long-term measures for integrating cybersecurity into governance, leveraging digital tools such as blockchain and AI to enhance transparency and accountability, and fostering international cooperation to mitigate cross-border threats. By fostering innovation and resilience, the findings offer a pathway to mitigating the socio-economic impacts of financial and cybercrimes and rebuilding stronger, more equitable systems in conflict-affected regions.

Keywords: financial fraud, cybercrime, corruption, shadow economies, post-war recovery, money laundering, national security, organized financial crime, economic governance, cybersecurity policies

JEL Classification: F52, H56, H56, K42, O33, Q01.

1st Edition

Range Range 187 pg (7.95 Signatures)

ISBN 978-3-911748-02-5

DOI: 10.61093/978-3-911748-02-5/2024