

TECHNOLOGY-ENABLED FRAUD IN THE DIGITAL ECONOMY: CRIMINOLOGICAL DETERMINANTS, VICTIMOLOGICAL VULNERABILITIES AND OFFENDER PROFILES

Sattarov Jasurbek Avazbekovich

Independent Researcher of Law Enforcement Academy
of the Republic of Uzbekistan

E-mail: jasur_sattarov@proacademy.uz

Abstract

This article examines cyber fraud committed through information technologies as a complex criminal-law, criminological, psychological, technological and victimological phenomenon. It argues that the digitalisation of economic relations has not merely changed the instruments of fraud, but has transformed the criminogenic environment in which fraudulent conduct is conceived, executed and concealed. Online lending, mobile banking, virtual cards, plastic card operations, instant money transfers, messengers and social networks have created new opportunities for offenders to exploit trust, urgency, financial need and digital illiteracy. The article rejects the narrow stereotype that the cyber fraud offender is necessarily a hacker or highly skilled programmer. In many cases, the offender acts as a social engineer, digital intermediary, fake official-status creator or opportunistic fraudster who manipulates the victim rather than technically breaking an information system. The research applies routine activity theory, the fraud triangle, rational choice theory, differential association theory, anomie theory and neutralisation theory to explain the causes and conditions of cyber fraud. It proposes authorial definitions of technology-enabled fraud, cyber fraud offender, digital-manipulative competence, illusion of officiality and digital criminogenic environment. The article concludes that effective prevention requires an integrated model combining criminal-law response, anti-fraud monitoring, digital literacy, victim-oriented reporting, interinstitutional cooperation and unified judicial practice.

Keywords: Cyber fraud, information technologies, digital criminology, offender personality, social engineering, online lending, virtual cards, victimology, anti-fraud systems, digital literacy, fraud triangle, routine activity theory.

Introduction

Fraud committed through information technologies has become one of the most significant challenges for contemporary criminal law and criminology. In the legal system of Uzbekistan, fraud is traditionally understood as the unlawful acquisition of another person's property or the right to such property by deception or abuse of trust [1]. The Plenum of the Supreme Court of the Republic of Uzbekistan has clarified that deception may consist not only in communicating false information, but also in concealing legally relevant facts that influence the victim's decision to transfer property or create conditions for its unlawful acquisition.[2] These classical legal elements remain conceptually important; however, the digital economy has substantially changed the factual form in which such deception is performed.

Traditional fraud was often based on direct interpersonal contact, oral promises, forged paper documents or personal abuse of trust. By contrast, technology-enabled fraud may occur through telephone calls, SMS messages, messengers, mobile banking applications, online credit platforms, virtual cards, social media profiles, digital payment systems and fake institutional communication. In these cases, information technologies do not always operate merely as neutral instruments. They may become part of the offence mechanism itself, enabling the offender to create a false appearance of legitimacy, obtain personal data, initiate financial transactions and rapidly withdraw or redirect funds.

The research problem addressed in this article is twofold. First, cyber fraud must be explained not only as a legal offence but also as a criminological phenomenon produced by the interaction of motivated offenders, vulnerable victims, weak digital guardianship and institutional gaps. Secondly, the personality of the cyber fraud offender requires a more nuanced analysis than the conventional image of a technically sophisticated hacker. Judicial practice shows that many offenders do not penetrate systems through advanced technical attacks. Instead, they use ordinary digital tools to manipulate trust, fear, urgency and financial need.

The purpose of this article is to develop an integrated criminological and legal analysis of cyber fraud committed through information technologies, with particular emphasis on its causes, conditions, victimological vulnerabilities and offender personality. The research objectives are: to analyse the digital transformation of fraud; to identify socio-economic, technological, psychological, institutional and victimological factors of cyber fraud; to examine the personality of the offender; to

construct a typology of cyber fraud offenders; to assess the role of social engineering; to evaluate relevant judicial practice; and to propose a comprehensive prevention model.

The methodological basis of the research includes doctrinal legal analysis, criminological analysis, victimological analysis, case-based analysis, system-structural method, behavioural analysis, digital-risk analysis and typological classification. The theoretical framework is based on routine activity theory [3], the fraud triangle,[4] rational choice theory [5], differential association theory [6], anomie theory [7] and techniques of neutralization [8].

Digital Transformation of Fraud as a Criminological Phenomenon

The digital transformation of fraud should not be understood as a simple replacement of old tools with new technologies. It represents a deeper change in the criminological environment of property crime. Mobile banking, online lending, virtual cards, electronic payment systems and messengers have created a transactional space in which deception can be carried out remotely, quickly and with reduced visibility. As David Wall argues, cybercrime is not only a technical category but also a transformation of crime in the information age, where technology reshapes opportunities, targets and control mechanisms [9].

Cyber fraud is simultaneously a property crime, a psychological manipulation, a technological abuse, a victimological phenomenon and an institutional-security problem. It is a property crime because its ultimate purpose is the unlawful acquisition of money, property rights or financial benefits. It is a psychological manipulation because the victim's decision-making process is influenced through fear, hope, urgency or trust. It is a technological abuse because digital systems are used to obtain data, create virtual cards, initiate online loans or redirect payments. It is victimological because the offender exploits low digital literacy, financial vulnerability and trust in official-looking communication. It is institutional because prevention depends on the coordinated response of banks, payment organisations, mobile operators, law enforcement agencies and courts.

The role of information technologies in cyber fraud is not uniform. In some cases, technology functions mainly as a communication channel: a phone call or messenger message is used to convince the victim to transfer money. In other cases, technology becomes the direct mechanism of the offence: personal data are obtained, an online

loan is issued, funds are credited to a virtual card and then transferred to the offender's plastic card. In a third group of cases, technology creates the appearance of lawful procedure: the offender imitates a bank employee, subsidy officer or public-service intermediary.

The criminological literature supports this broader understanding. Yar and Steinmetz argue that cybercrime must be analysed as a relationship between technology, social behaviour and systems of control.[10] Holt and Bossler similarly note that technology-enabled offences require the adaptation of traditional criminological theories to online and digitally mediated environments [11]. This is particularly true of fraud, where the victim's trust is mediated through a platform, application, digital document or institutional symbol.

Accordingly, technology-enabled fraud may be defined as an intentional property-related offence in which information technologies, digital communication channels, online financial instruments or digital identity mechanisms are used to deceive a person, abuse trust, exploit vulnerability or manipulate a transaction in order to obtain unlawful financial or property-related benefit.

Causes and Conditions of Cyber Fraud

A precise criminological analysis requires a distinction between causes and conditions. Causes generate or strengthen criminal motivation, whereas conditions facilitate the realisation of that motivation. In cyber fraud, these two dimensions are closely connected but should not be confused.

Socio-economic factors

The first group of causes consists of socio-economic factors. Unemployment, temporary lack of income, debt, family financial pressure, informal income-seeking and the desire for quick profit may strengthen criminal motivation. However, economic hardship alone does not explain fraud. Merton's anomie theory is useful here because it shows how socially approved goals, especially material success, may produce deviant adaptations when lawful means are perceived as limited.[12] Yet this theory must be applied cautiously: many individuals face financial hardship without committing crime. Economic pressure becomes criminogenic only when it combines with opportunity, weak moral restraints and rationalisation.

The victim's socio-economic condition is also relevant. A person who urgently needs credit, subsidy, employment, border-crossing assistance or administrative support

may become more susceptible to fraudulent offers. This does not shift responsibility to the victim. Rather, it demonstrates that offenders deliberately identify and exploit economically sensitive situations.

Technological Factors

The second group of conditions consists of technological factors. Online lending, instant transfers, virtual cards, mobile banking, weak remote identification, insufficient transaction monitoring and rapid cash-out mechanisms create opportunities for fraud. In the logic of routine activity theory, the digital environment brings together a motivated offender, a suitable target and weak guardianship [13]. The suitable target may be a user of mobile banking who lacks knowledge of security rules. Weak guardianship may take the form of insufficient biometric verification, delayed transaction alerts or inadequate anti-fraud algorithms.

This explains why virtual cards and online credit platforms are particularly vulnerable. If an offender obtains personal data and uses them to initiate a loan, the transaction may be processed before the victim understands its legal consequences. Newman and Clarke's work on e-commerce crime is relevant here because it stresses the importance of designing opportunity-reduction mechanisms into digital commercial systems [14].

Psychological Factors

The third group consists of psychological factors. Cyber fraud frequently relies on urgency, fear, hope, authority and reduced critical thinking under pressure. Offenders use phrases equivalent to "today is the last day", "send documents immediately", "pay now", "your issue will be resolved", "your credit limit has not been approved" or "there is a restriction on you". These expressions are not accidental. They are behavioural tools designed to limit verification and induce compliance.

The fraud triangle, initially developed by Cressey and later expanded by Albrecht and co-authors, explains fraudulent behaviour through pressure, opportunity and rationalization [15]. In cyber fraud, pressure may arise from financial need; opportunity is provided by digital systems and victim vulnerability; rationalisation appears when offenders justify their conduct by claiming that the victim trusted them voluntarily or that they intended to return the money later.

Institutional Factors

Institutional conditions also play a decisive role. If banks, payment organisations, mobile operators, digital platforms, law enforcement bodies and courts do not exchange information rapidly, offenders benefit from institutional fragmentation. Gercke emphasises that cybercrime prevention requires not only substantive criminal-law norms but also effective procedural and institutional mechanisms for detecting, preserving and exchanging digital evidence [16].

In the context of Uzbekistan, this implies that cyber fraud prevention cannot rely solely on post-crime investigation. It must include real-time monitoring, rapid freezing of suspicious transfers, preservation of electronic traces and standardised cooperation between financial institutions and law enforcement agencies.

Victimological Factors

Victimological factors include low digital literacy, low financial literacy, negligent disclosure of personal data, inability to verify official status, trust in institutional language and delayed reporting after victimisation. Button and Cross argue that fraud victimology should not be reduced to blaming victims, but should explain how emotional, financial and informational vulnerabilities are exploited by offenders [17]. Victimological vulnerability in cyber fraud may therefore be defined as a condition in which a person's financial need, lack of digital knowledge, trust in official-looking communication, emotional pressure or inability to verify information is intentionally exploited by an offender through technological or social-engineering means.

The Personality of the Cyber Fraud Offender

The cyber fraud offender cannot be adequately understood through the narrow stereotype of a hacker or programmer. While some offenders may possess advanced technical skills, many rely on moderate digital competence combined with psychological manipulation. Brenner notes that cybercrime often involves the adaptation of traditional criminal behaviour to new technological settings rather than wholly new forms of deviance [18]. Clough similarly emphasises that cybercrime law must address both technical conduct and human-mediated misuse of digital systems [19].

Cyber fraud offenders do not belong to a single socio-demographic category. They may be unemployed, temporarily unemployed, formally employed, previously

unconvicted, professionally connected to a relevant sector or capable of imitating institutional authority. The important criminological point is that the offender's dangerousness may derive not from advanced information-technology education but from the ability to combine ordinary digital tools with deception.

Uzbek criminological studies also support this broader approach. Altiev argues that fraud must be studied as a complex phenomenon involving the offender's personality, motivation, social environment, victim vulnerability and prevention mechanisms [20]. Kh.Ochilov, analysing computer-related theft of another's property, connects such offences with the expansion of information technologies, non-cash payments and changing forms of property crime [21]. These approaches are especially relevant to online credit fraud, virtual-card schemes and mobile-application-based deception.

The offender's motivation is usually centred on unlawful financial gain. Nevertheless, this motivation may be reinforced by debt, low perceived risk, unemployment, opportunism, expectation of anonymity and the possibility of rapidly cashing out funds. Cornish and Clarke's rational choice theory explains this conduct as a calculated decision in which the offender evaluates expected benefits, risks and costs [22].

In cyber fraud, the offender may calculate that the victim will trust quickly, the money can be transferred instantly, reporting will be delayed and the phone number or account can be abandoned. Levi's analysis of long-firm fraud is also instructive because it shows how fraudsters organise deception around delayed detection and exploitation of trust in commercial relations [23].

The moral-psychological characteristics of the cyber fraud offender include manipulative thinking, readiness to exploit trust, low empathy, instrumental attitude toward victims and rationalisation of misconduct. Sykes and Matza's neutralisation theory explains how offenders deny responsibility, minimise harm, blame the victim or appeal to necessity [24]. In cyber fraud, similar rationalisations may appear in claims such as "I only mediated", "the victim trusted me", "the damage was not serious" or "I intended to return the money".

Such rationalisation increases the risk of repeated offending. If the offender psychologically reframes the act as mediation, a temporary borrowing or a minor deception, the barrier to repeating the same scheme is reduced.

The digital-behavioural profile of the cyber fraud offender includes the ability to use mobile applications, online lending systems, virtual cards, messengers, fake accounts, card-to-card transfers, voice messages and screenshots for criminal purposes. This may be described as digital-manipulative competence.

Digital-manipulative competence is the practical ability of an offender to combine digital instruments with psychological influence in order to obtain personal data, simulate legitimacy, initiate financial transactions, redirect funds or conceal the unlawful character of an operation.

This competence has two levels. The first is technical-computer competence, involving interference with systems or data. The second is socio-technological competence, involving the use of lawful digital tools to manipulate the victim. In many cases, the second level is more common and more practically dangerous.

Social engineering is one of the most important behavioural characteristics of the cyber fraud offender. Grabosky's analysis of electronic crime shows that technological offences frequently depend on human conduct, weak guardianship and trust-based vulnerabilities [25]. In the same vein, many cyber fraud offenders do not technically breach a system; they induce the victim to operate the system in the offender's interest.

The offender creates an illusion of officiality by using institutional vocabulary, references to banks, subsidies, customs authorities, inspections, debts, service fees, credit limits or legal restrictions. The illusion of officiality may be defined as a deliberately constructed digital or communicative appearance of institutional legitimacy through which the offender induces the victim to trust the communication, disclose information, transfer money or perform another legally significant action.

Typology of Cyber Fraud Offenders

A typology of cyber fraud offenders is necessary for differentiated prevention. The following types may be identified.

First, the digital intermediary offender uses mobile banking, online lending, virtual cards and plastic card operations to obtain unlawful benefit. This type is particularly visible in online credit fraud, where the offender obtains the victim's data, initiates a loan and transfers the credited funds to another card [26].

Secondly, the social engineer offender relies primarily on psychological influence. His tools are urgency, fear, authority simulation, hope and manipulation of trust. This type is central to phone-based, messenger-based and subsidy-related fraud.

Thirdly, the fake official-status creator presents himself as a bank employee, dealer, subsidy officer, customs intermediary, public-service representative or other official actor. The offender's social role is false, but the victim perceives it as institutionally credible [27].

Fourthly, the opportunistic fraudster exploits situational vulnerability. For example, a person urgently needing to cross a border, obtain a document or resolve an administrative problem may be induced to pay money to someone claiming to have "connections" [28].

Fifthly, the repeated-scheme fraudster uses the same scenario against multiple victims. This type reflects Sutherland's differential association theory: fraudulent techniques may be learned, repeated and transmitted within social groups [29].

Sixthly, the role-distributed group fraudster participates in a coordinated scheme where one person communicates with victims, another receives money, a third cashes out funds, and another provides digital infrastructure. Tropina's work on cybercrime and organised criminality is relevant because it demonstrates that digital offences often combine technical tools with networked criminal roles [30].

Victimological Vulnerability in Cyber Fraud

Victimological analysis must not be used to blame the victim. Its proper function is to identify how offenders exploit vulnerabilities and how prevention may reduce victimisation. Victims of cyber fraud often act under urgency, uncertainty, economic need or institutional trust. They may believe that a bank, subsidy organisation or public authority is contacting them.

Low digital literacy is a major vulnerability. A victim may not understand the legal consequences of sharing passport data, SMS codes, card details, screenshots or mobile-banking information. Low financial literacy is equally important: victims may not distinguish between a lawful administrative fee and a fraudulent prepayment, between a real subsidy process and a fabricated one, or between a genuine bank verification and a fraudulent request.

Button and Cross argue that fraud victims often experience shame and delayed reporting, which further benefits offenders [31]. Therefore, victim-oriented

prevention must reduce stigma and create rapid reporting channels. Citizens should be given practical instructions: bank employees do not request SMS codes; subsidies are not obtained through prepayment to private plastic cards; online credit must be confirmed only by the person concerned; and promises to “resolve matters through acquaintances” are typical fraud indicators.

Judicial practice provides important empirical material for understanding cyber fraud. One group of cases concerns online credit fraud through mobile banking. In a judgment dated 20 May 2024, the offender presented himself as connected with a bank, obtained victims’ personal data, initiated online credit transactions, directed money to virtual cards and then transferred funds to his own plastic card [32]. The criminological significance of this model lies in the combination of digital-manipulative competence and victimological vulnerability.

Another model concerns fake subsidy-related fraud. In a judgment dated 22 July 2024, the offender presented himself as an employee of a subsidy organisation, promised financial assistance to fish-farming enterprises and demanded a “1% service fee”, after which he disappeared [33]. Here the key mechanism was not technical intrusion, but the construction of official appearance and exploitation of economic expectation. A third model concerns the creation of fake authority through telephone communication. In a judgment dated 4 October 2024, the offender used his connection with an electricity-related institution to convince a farmer that there was a debt or inspection issue and offered to resolve it for money [34]. This case demonstrates that information technology may function as a psychological communication channel rather than a direct financial mechanism.

These cases confirm that cyber fraud should be studied through behavioural models rather than only through technical means. The decisive question is how the offender combines communication, trust, digital tools and financial movement.

Prevention of Cyber Fraud

Prevention of cyber fraud must be multidimensional. Criminal-law prevention requires proper qualification, inevitability of liability and unified judicial guidance. Courts and investigators need methodological recommendations on digital evidence, offender typology and the distinction between civil-law disputes and criminal fraud. Banking and financial prevention must include stronger anti-fraud algorithms, real-time transaction monitoring, suspicious operation blocking, biometric verification,

risk scoring and instant customer alerts. McGuire and Dowling's review of cybercrime evidence confirms that cyber-enabled fraud requires responses that address both technological opportunity and behavioural manipulation [35].

Digital literacy and financial education must be practical rather than abstract. Citizens should be taught how online credit operates, why SMS codes should not be disclosed, how to verify official status, why service fees should not be sent to private cards and how to report suspicious communication immediately.

Victim-oriented prevention must reduce shame and encourage early reporting. Emergency freezing of suspicious transfers should be made accessible. Interinstitutional cooperation between banks, payment systems, mobile operators, cybercrime units, prosecutors, courts and preventive bodies should be strengthened. Digital profiling should identify repeated phone numbers, bank cards, narratives, victim categories and transaction patterns.

Conclusion

Cyber fraud committed through information technologies is not merely traditional fraud transferred to the internet. It is a complex criminological phenomenon in which digital infrastructure, psychological manipulation, financial technology, victim vulnerability and institutional weakness interact. The offender may be a digital intermediary, social engineer, fake official-status creator, opportunistic fraudster, repeated-scheme offender or member of a role-distributed group.

The main danger of the cyber fraud offender often lies not in advanced technical ability, but in the capacity to exploit human trust through digital tools. Such offenders use urgency, fear, hope, institutional vocabulary, fake official status and digital payment mechanisms to achieve unlawful financial results.

Effective prevention requires a model that protects both the technical system and the human decision-making process. Criminal-law response is necessary, but insufficient. It must be combined with anti-fraud monitoring, biometric verification, digital literacy, victim-friendly reporting, rapid freezing of suspicious transfers, interinstitutional cooperation and unified judicial practice.

References

1. Criminal Code of the Republic of Uzbekistan. — National Database of Legislation of the Republic of Uzbekistan. — URL: <https://lex.uz/acts/111453>

2. Resolution No. 17 of the Plenum of the Supreme Court of the Republic of Uzbekistan “On Judicial Practice in Fraud Cases”, 23 June 2023. — URL: <https://lex.uz/docs/6523582>
3. Cohen L.E., Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach // American Sociological Review. — 1979. — Vol. 44. — No. 4. — P. 588–608.
4. Cressey D.R. Other People’s Money: A Study in the Social Psychology of Embezzlement. — Glencoe, Illinois: Free Press, 1953. — P. 33–47, 159–166.
5. Cornish D.B., Clarke R.V. The Reasoning Criminal: Rational Choice Perspectives on Offending. — New York: Springer-Verlag, 1986. — P. 1–16, 147–185.
6. Sutherland E.H. White Collar Crime. — New York: Dryden Press, 1949. — P. 9–20, 227–248.
7. Merton R.K. Social Structure and Anomie // American Sociological Review. — 1938. — Vol. 3. — No. 5. — P. 672–682.
8. Sykes G.M., Matza D. Techniques of Neutralization: A Theory of Delinquency // American Sociological Review. — 1957. — Vol. 22. — No. 6. — P. 664–670.
9. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. — Cambridge: Polity Press, 2007. — P. 1–28, 53–78.
10. Yar M., Steinmetz K.F. Cybercrime and Society. — 4th ed. — London: SAGE Publications Ltd, 2023. — P. 1–40, 151–190.
11. Holt T.J., Bossler A.M. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. — London; New York: Routledge, 2016. — P. 1–25, 165–203.
12. Merton R.K. Social Structure and Anomie // American Sociological Review. — 1938. — Vol. 3. — No. 5. — P. 672–682.
13. Cohen L.E., Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach // American Sociological Review. — 1979. — Vol. 44. — No. 4. — P. 588–608.
14. Newman G.R., Clarke R.V. Superhighway Robbery: Preventing E-commerce Crime. — Portland, Oregon: Willan Publishing, 2003.
15. Albrecht W.S., Albrecht C.O., Albrecht C.C., Zimbelman M.F. Fraud Examination. — 6th ed. — Boston: Cengage Learning, 2018.

16. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. — Geneva: International Telecommunication Union, 2012. — P. 73–91.
17. Button M., Cross C. Cyber Frauds, Scams and Their Victims. — London; New York: Routledge, 2017. — DOI: 10.4324/9781315679877.
18. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. — Santa Barbara, California: Praeger, 2010.
19. Clough J. Principles of Cybercrime. — Cambridge: Cambridge University Press, 2015.
20. Altiev R.S. Firibgarlikning jinoyat-huquqiy va kriminologik jihatlari: yuridik fanlar bo'yicha falsafa doktori (PhD) dissertatsiyasi. — Toshkent: Toshkent davlat yuridik universiteti, 2020. — B. 95–146.
21. Ochilov H.R. O'zgarlar mulkini kompyuter vositalaridan foydalanib talon-toroj qilganlik uchun javobgarlik: yuridik fanlar bo'yicha falsafa doktori (PhD) dissertatsiyasi. — Toshkent: Toshkent davlat yuridik universiteti, 2017. — B. 3–12, 132–166.
22. Cornish D.B., Clarke R.V. The Reasoning Criminal: Rational Choice Perspectives on Offending. — New York: Springer-Verlag, 1986. — P. 1–16.
23. Levi M. The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud. — Aldershot: Ashgate, 2008. — P. 1–35, 285–330.
24. Sykes G.M., Matza D. Techniques of Neutralization: A Theory of Delinquency // American Sociological Review. — 1957. — Vol. 22. — No. 6. — P. 664–670.
25. Grabosky P. Electronic Crime. — Upper Saddle River, New Jersey: Prentice Hall, 2007.
26. Judgment of the District Criminal Court dated 20 May 2024, case No. 1-1209-2401/49.
27. Judgment of the District Criminal Court dated 22 July 2024, case No. 1-1209-2401/79.
28. Judgment of the District Criminal Court dated 19 June 2024, case No. 1-1208-2401/140.
29. Sutherland E.H. White Collar Crime. — New York: Dryden Press, 1949. — P. 9–20, 227–248.
30. Tropina T. Cybercrime and Organised Crime: New Challenges for Criminal Law // Selected academic publications on cybercrime and criminal law.

31. Button M., Cross C. Cyber Frauds, Scams and Their Victims. — London; New York: Routledge, 2017. — DOI: 10.4324/9781315679877.
32. Judgment of the District Criminal Court dated 20 May 2024, case No. 1-1209-2401/49.
33. Judgment of the District Criminal Court dated 22 July 2024, case No. 1-1209-2401/79.
34. Judgment of the District Criminal Court dated 4 October 2024, case No. 1-1207-2401/106.
35. McGuire M., Dowling S. Cyber Crime: A Review of the Evidence. Research Report 75. — London: Home Office, 2013. — Vol. 1: Cyber-dependent crimes; Vol. 2: Cyber-enabled crimes.