

CYBERCRIME AMONG YOUNG PEOPLE IN ALBANIA: SOCIAL LEARNING, DIGITAL COMMUNITIES AND CRIMINAL OPPORTUNITY

MSc. Alberjana Murati

Faculty of Political Sciences and Law, Department of Law, “Aleksandër Moisiu” University, Durrës, Albania

Abstract: This article aims to develop an Albania-specific framework for understanding how young people may become involved in cyber-offending. It brings together social learning theory and criminal opportunity perspectives to explain how digital communities, peer influence, technical learning and online opportunities can shape pathways toward unlawful conduct. The article examines Albanian criminal law, cybersecurity policy and relevant international research through a structured narrative review and doctrinal-policy analysis. It seeks to distinguish ordinary digital participation and technical competence from criminal behaviour, while identifying the conditions under which skills and online interactions may be directed toward cyber-offending. The analysis also aims to clarify the limits of the available Albanian evidence and to establish a foundation for future national research. On this basis, the article proposes an integrated explanatory model and outlines preventive responses centred on cyber ethics, legitimate technical development, early intervention, proportionate diversion and improved data collection. Its central argument is that technical competence should be treated as a social asset whose direction depends on learning environments, available opportunities and forms of recognition.

Keywords: youth cybercrime; social learning theory; digital communities; criminal opportunity; cyber-dependent crime; Albania; prevention

1. Introduction

Cybercrime unsettles familiar criminological boundaries. The conduct may be committed from a bedroom rather than a street, the victim may be in another jurisdiction, and the relevant peer group may never meet physically. A young person can move quickly from ordinary gaming, coding or social-media use to a specialised forum, channel or server. In these spaces, unauthorised access, credential theft, denial-of-service attacks, fraud or malicious software may be presented as games, services or signs of competence. The digital setting does not abolish social influence; it reorganises it. Peers become searchable, tutorials persist, audiences are scalable, reputation is quantified and technical opportunities can be tested with comparatively little immediate visibility.

The Albanian context makes this question timely. INSTAT reported that in 2025, 87.2 per cent of persons aged 16–74 used the internet and 97.3 per cent of users accessed it several times a day. Mobile phones were used for internet access by 99.9 per cent of users, while participation in social networks continued to increase. The same survey recorded growth in digital skills. The share of people who reported that they could write code rose from 8.7 per cent in 2024 to 11.2 per cent in 2025. These developments are socially and economically positive. They enlarge education, participation and employment. They also mean that opportunity, peer contact and technical experimentation increasingly occur in the same digital spaces (INSTAT, 2025).

Official criminal-justice statistics require more cautious interpretation. INSTAT recorded 38,345 criminal offences in 2025. This was 17.4 per cent more than in 2024. It classified cybercrime by reference to unauthorised access, illegal interception, interference with data or systems, and misuse of equipment. Cybercrime as a recorded category decreased by 18.8 per cent from 2024 to 2025. That movement cannot be treated as a measure of youth cyber-offending. Recorded crime depends on victim reporting, institutional detection, legal

classification, investigative capacity and cross-border evidence, and the published headline series does not provide a youth-by-cyber-offence cross-tabulation (INSTAT, 2026).

This article asks a narrower and more defensible question than whether Albanian youth are becoming ‘cybercriminals’. It asks how social learning and criminal opportunity may explain youth cyber-offending. It also examines what the available Albanian evidence can establish. Finally, it considers how prevention can protect legitimate technical development while interrupting harmful conduct. The article treats young people as a diverse social group, not as a suspect class. It distinguishes cyber-dependent offences from cyber-enabled offences. Cyber-dependent offences can exist only through information systems. In cyber-enabled offences, technology increases the scale or reach of conventional crime.

For this study, ‘young people’ refers primarily to persons aged 14–24. The lower boundary reflects the minimum age of criminal responsibility for ordinary offences under Albanian law. The upper boundary covers the transition from adolescence to early adulthood. This age range is common in youth-crime research. The legal analysis maintains a clear distinction between minors and young adults. Minors aged 14–17 benefit from the special guarantees of the Code of Criminal Justice for Children. Young adults aged 18–24 are generally subject to the adult criminal process. Evidence using different age bands is identified as such and is not treated as directly comparable.

The article’s original contribution is threefold. First, it separates digital exposure from cyber-offending and thereby avoids treating connectivity or coding ability as proxies for criminality. Second, it links social learning to opportunity through a staged model in which association and definitions influence motivation, capability enables execution, opportunity supplies a target, and reinforcement shapes repetition. Third, it converts Albania’s statistical fragmentation into a research finding: the absence of age-by-offence and pathway data limits both causal explanation and evaluation of prevention.

2. Research Questions and Methodological Approach

The aim is to construct an Albania-specific explanatory and preventive framework for youth cyber-offending. Four research questions guide the inquiry. First, how can digital communities influence the start and continuation of cyber-offending through social learning? Second, how do online routines and technical features create criminal opportunities? Third, what does current Albanian evidence reveal, and where are its main gaps? Fourth, which preventive and criminal-justice responses follow from the combined framework?

The study combines a structured narrative review, doctrinal legal analysis and a policy-focused Albanian case study (Snyder, 2019). Searches were conducted from 24 August to 10 September 2026 in Google Scholar and Crossref-linked publisher databases. Official repositories of INSTAT, the General Prosecutor, the Albanian National Cybersecurity Authority, the Council of Europe, the European Commission and Europol were also searched. Search strings combined ‘youth cybercrime’, ‘juvenile cyber-deviance’, ‘social learning’, ‘differential association’, ‘digital communities’, ‘routine activity’, ‘criminal opportunity’, ‘cyber-dependent crime’ and ‘Albania’. Backward citation searching identified foundational theory and leading empirical studies. The final bibliography contains 31 academic, legal and institutional sources. It records the sources used in the synthesis rather than every item returned by the searches.

Peer-reviewed studies were included when they examined offending or closely related cyber-deviance among minors, students or young adults and analysed social-learning, peer, capability, self-control or opportunity variables. Foundational works were retained for conceptual development. Official sources were included when they supplied binding law, Albanian administrative data, policy commitments or institutional assessments. Duplicate summaries, commentary without identifiable methods and prevalence claims without a defined population were excluded. Sources were screened for relevance to the research questions, population, conduct

and evidential quality. Heterogeneity in offences, age bands, measures and research design made statistical pooling inappropriate, so the evidence was synthesised narratively.

The method is explanatory and doctrinal; it does not estimate prevalence or test causation in Albania. No representative Albanian self-report study located for this review measures specific cyber-offences together with peer association, favourable definitions, technical capability, guardianship and reinforcement. International studies are therefore used to identify plausible mechanisms and derive propositions for national testing, not to import foreign prevalence rates or effect sizes. Albanian administrative statistics describe reported, detected and legally classified events. They cannot measure undetected conduct or explain individual pathways.

The search prioritised English and Albanian materials published from 2010 onward, while older works were included when foundational. The review was not registered, did not use a formal risk-of-bias instrument and could not examine inaccessible Albanian case files. These choices limit reproducibility and the strength of causal inference. The article must therefore be read as a structured narrative review and doctrinal-policy analysis that constructs an Albania-specific model for future testing, not as a PRISMA-compliant systematic review or an empirical study of Albanian offenders.

3. Theoretical framework

3.1. Social learning in digital environments

Sutherland's differential association theory proposes that criminal conduct is learned through communication and that offending becomes more likely when definitions favourable to law violation outweigh definitions favourable to conformity. Associations vary in frequency, duration, priority and intensity (Sutherland, 1947). Bandura's account of observational learning further clarifies how attention, retention, reproduction and anticipated consequences affect imitation (Bandura, 1977). Burgess and Akers connected this proposition to reinforcement, while Akers later organised social learning around differential association, definitions, imitation and differential reinforcement (Burgess and Akers, 1966; Akers, 1998). The theory does not claim that contact automatically produces crime. It predicts that influence is stronger when the source is credible, repeated and socially significant and when conduct appears rewarded.

Digital communities modify each element. Association can occur through public videos, private channels, gaming groups, code repositories and specialised forums. Definitions may frame unauthorised access as harmless exploration, piracy as normal sharing, fraud as retaliation against wealthy institutions, or disruption as proof of skill. Imitation is facilitated when scripts and demonstrations can be copied. Reinforcement may be material, but it can also consist of attention, rank, access to restricted groups, technical recognition or the satisfaction of solving a difficult problem. Research applying the full social-learning model shows that its combined elements explain substantial variation in cyber-deviance. Research on young people also identifies deviant peer association as a significant correlate (Holt, Burruss and Bossler, 2010; Holt, Bossler and May, 2012).

The distinction between online content and online community is essential. A tutorial can supply information without trust, feedback or identity. A community can supply all four: it interprets the act, validates the learner, corrects errors and determines whether competence earns status. Bekkers, Holt and Leukfeldt studied 1,240 young people in the Netherlands. Serious cyber-dependent conduct was closely linked to social-learning environments and technical capability. For simpler conduct, the apparent role of self-control became weaker after learning variables were included (Bekkers, Holt and Leukfeldt, 2026). The implication is not that the Dutch estimates apply to Albania, but that complex cyber-offending may require a social and technical ecology rather than impulsivity alone.

3.2. Criminal opportunity and online routine activity

Routine activity theory explains crime through the convergence of a motivated offender, a suitable target and the absence of capable guardianship (Cohen and Felson, 1979). In cyberspace, convergence is not physical. Targets can be persistently reachable; credentials can be reused across services; automated tools can scan at scale; and guardianship is distributed among users, parents, schools, platforms, service providers, cybersecurity teams and police. Opportunity theory adds what social learning alone cannot: even a favourable definition and acquired skill may not become an offence unless a target is accessible and perceived risk is manageable.

The two perspectives are complementary. Social learning explains how a young person comes to recognise an opportunity as meaningful, legitimate within a peer group and technically executable. Routine activity explains when systems, users or transactions become available with insufficient protection. The interaction follows a sequence. It starts with exposure to peers or content. The person may then reinterpret legal and moral boundaries, acquire a tool, and encounter a vulnerable target. Feedback and reward can encourage repetition or specialisation.

This sequence also explains why broad internet penetration should never be equated with criminality. Connectivity increases the number of lawful activities far more than criminal acts. Risk arises from particular combinations: unstructured time, deviant association, accessible tools, favourable definitions, weak guardianship and an exploitable target. Conversely, the same access can strengthen guardianship through education, reporting, peer support and legitimate cybersecurity communities.

3.3. Testable propositions

The integrated framework produces four propositions suitable for national testing. Proposition 1: association with deviant online peers will be positively related to cyber-offending primarily when it is accompanied by definitions favourable to unauthorised conduct. This follows social-learning meta-analytic evidence showing that association and definitions are among the most consistent predictors of offending (Pratt et al., 2010). Proposition 2: technical capability will strengthen the relationship between favourable definitions and serious cyber-dependent offending because complex conduct requires more than willingness.

Proposition 3: capable digital guardianship—including clear school rules, secure system design, parental communication and responsive platform moderation—will weaken the relationship between exposure and offending opportunity. Proposition 4: access to legitimate recognition, mentoring and cybersecurity employment will reduce the reinforcing value of deviant digital communities. These propositions distinguish mediation, moderation and substitution. They also make the article falsifiable: Albanian data may show that one mechanism is weak, limited to particular offences or outweighed by selection effects.

The propositions should be tested with behaviour-specific measures. Password guessing, unauthorised access, denial-of-service activity, malware development, computer fraud and account-based facilitation should not be collapsed into a single binary outcome. Zhou's study of offending versatility suggests that traditional social-learning measures may operate differently across cyber-enabled and cyber-dependent offending, reinforcing the need for disaggregated analysis (Zhou, 2024).

3.4. Neutralisation, capability and escalation

Techniques of neutralisation help explain how young users suspend ordinary legal commitments without adopting a stable criminal identity. Several neutralisations are possible. The person may deny harm because data were copied rather than physically taken. The victim may be blamed for weak security. Responsibility may be attributed to a group challenge. The act may also be presented as educational testing (Sykes and Matza, 1957). Some justifications contain a partial truth—weak security exists, and ethical testing is valuable—but the inference that this authorises access is legally and ethically false.

Capability separates intention from execution. Basic password guessing or use of a preconfigured stressor service demands less knowledge than developing malware, maintaining infrastructure or laundering proceeds. Capability can be acquired legitimately and used unlawfully, or acquired inside a criminal setting from the outset. Progression is not inevitable. Europol's youth-pathways work emphasises that interest in technology can develop toward lawful cybersecurity or harmful conduct depending on personal, social and environmental conditions (Europol, 2017). Prevention should therefore identify turning points before identity and income become dependent on offending.

4. Albania's digital and criminological context

4.1. Connectivity, skill and exposure

Albania's digital transition creates a dense environment of everyday exposure. Internet and smartphone use is high. In addition, 99.5 per cent of the surveyed population aged 16–74 reported having an account on the e-Albania platform. A further 45.4 per cent had made online purchases during the previous twelve months (INSTAT, 2025). Digital public services and commerce increase convenience and state capacity, but they also enlarge the practical importance of credentials, identity data, payment information and trusted communications. Young people enter this environment not as peripheral users but often as family intermediaries with greater technical fluency.

Digital skill is protective and productive. It improves employability, enables scrutiny of suspicious content and supplies the workforce required for national resilience. Yet skill without ethics, mentoring or lawful challenge can be recruited into informal markets. The National Cybersecurity Strategy 2025–2030 recognises this duality. It gives priority to the online protection of citizens, especially children and young people. It also promotes cyber ethics, public awareness and professional capacity. Other priorities include research, mentoring, innovation and cooperation among universities, public institutions and the private sector (Council of Ministers of Albania, 2025). This policy architecture provides a basis for criminologically informed prevention, but its effect will depend on implementation and measurement.

A central risk in public debate is moral panic. Young people who code, use privacy tools, participate in gaming communities or explore system design should not be treated as presumptive offenders. Such labelling can damage trust and push technically interested youth away from institutions. The appropriate object of assessment is behaviour and context: authorisation, intent, harm, persistence, concealment, peer pressure, financial motive and connection to organised actors.

4.2. Recorded cybercrime and the data gap

INSTAT's 2025 criminal-justice publication defines cybercrime consistently with Directive 2013/40/EU (European Parliament and Council, 2013) and Albanian provisions on unauthorised access, illegal interception, data interference, system interference and misuse of equipment. The category's recorded decrease of 18.8 per cent in 2025 follows the logic of police recording and cannot independently show a fall in underlying offending. Victims may not detect intrusion; organisations may manage incidents without criminal complaints; conduct may be recorded as fraud or another offence; and evidence may be located abroad.

4.3. Prosecution evidence and its limits

The General Prosecutor's annual report materially improves the description of recorded cybercrime. In 2025, cybercrime represented 0.76 per cent of all registered proceedings and the report calculated a rate of 8.72 proceedings per 100,000 inhabitants. Table 35 records 206 cybercrime proceedings in 2025, down from 303 in 2024; 17 proceedings were sent to trial, 29 defendants were registered, 24 defendants were sent to trial and 22 were convicted. Computer fraud under Article 143/b was the largest category, with 81 registered proceedings.

Computer forgery under Article 186/a followed with 70 proceedings. Interference with computer data under Article 293/b accounted for 41 proceedings (General Prosecutor of Albania, 2026).

These figures describe different stages of legal processing, not a single annual cohort and not the size of the underlying phenomenon. Proceedings registered, defendants registered, cases sent to trial and convictions may concern files initiated or completed in different years. One proceeding may contain several incidents or defendants, while several reports may be consolidated. The fall in registered proceedings alongside increases in registered and convicted defendants can therefore reflect case complexity, procedural timing, charging choices, consolidation or institutional capacity. It cannot establish either a decline or an increase in underlying cyber-offending without file-level and cohort-based analysis.

The same report separately states that 1,096 proceedings involving minors in conflict with the law were registered in 2025, including 961 minors recorded as defendants or persons under investigation. Diversion was applied in 521 discontinued cases involving 534 minors. The report does not disclose how many of those minors were involved in cybercrime. The scientifically correct conclusion is therefore not that Albania had a specified number of juvenile cyber-offenders, but that two valuable datasets remain unlinked. This absence prevents calculation of age-specific cybercrime rates and evaluation of diversion for cyber-offences.

The data also illustrate the problem of offence boundaries. Many digitally mediated acts appear under computer fraud, computer forgery, unauthorised access or data interference, while other online conduct can be recorded under ordinary fraud, threats, sexual offences or offences against children. A youth cybercrime dataset must therefore combine legal classification with *modus operandi* rather than relying on a single chapter heading.

More importantly, aggregate data do not show how many suspects were minors or young adults. They do not identify each person's role or learning pathway. They also do not show whether an online community was involved or what outcome followed. Albania therefore lacks a publicly visible learning-oriented evidence chain connecting incident, age, motivation, peer context, skill source, legal disposition and recidivism. This is a substantive policy limitation. Prevention cannot be evaluated if authorities know the number of files but not the pathways represented by those files.

Future measurement should link anonymised police, prosecution, court and diversion data while preserving data-protection safeguards. A periodic representative self-report study could ask about specific behaviours rather than the ambiguous label 'hacking'; perceived legality; peer conduct; online communities; victimisation; parental and school guardianship; technical ability; rewards; and desistance. Longitudinal or repeated designs would better distinguish influence from selection.

4.4. Albanian criminal law and juvenile justice

4.4.1. Sources and limits of criminal liability

Albania is a Party to the Budapest Convention. Its domestic framework combines the Criminal Code, the Criminal Procedure Code, the Code of Criminal Justice for Children, cybersecurity regulation, data-protection law and international cooperation instruments. These bodies of law serve different purposes. Criminal liability must be based on a defined offence and proved against the individual. Cybersecurity duties regulate organisational resilience and incident management. Procedural rules govern how electronic evidence is preserved, obtained and tested. Juvenile justice adds specialised guarantees and developmentally appropriate responses.

The principle of legality requires conduct to fall within the elements of a criminal offence. Technical competence, possession of ordinary dual-use software, participation in a digital forum or knowledge of a vulnerability is not sufficient by itself. Investigators must prove the prohibited act, the required mental element and the person's individual contribution. In practice, the central distinctions are between authorised and

unauthorised conduct, preparation and attempt, mere presence and participation, and technical assistance given knowingly or without awareness of the criminal plan.

4.4.2. Substantive computer-related offences

The Criminal Code addresses both cyber-dependent and cyber-enabled conduct. Article 192/b criminalises unauthorised access to a computer system. Article 293/a concerns unlawful interception of non-public computer-data transmissions. Article 293/b protects computer data against unauthorised damaging, alteration, deletion or suppression, while Article 293/c addresses serious interference with the functioning of a computer system. Article 293/ç concerns the production, possession, sale, distribution or making available of devices, computer programmes, passwords or access codes for criminal use. Article 143/b addresses computer fraud and Article 186/a computer forgery. Other offences, including ordinary fraud, threats, sexual offences, money laundering and offences against children, may apply when technology enables rather than constitutes the conduct (Republic of Albania, 1995, as amended).

The legal classification must follow the protected interest and the concrete conduct. Guessing or using another person's password may constitute unauthorised access when it crosses a protected boundary without permission. Altering data or disrupting a service may trigger different provisions and may coexist with access liability. Computer fraud requires more than access: it requires manipulative conduct connected to unlawful economic benefit and loss. Computer forgery concerns the authenticity or legal use of computer data. The same digital episode may therefore contain several acts, but cumulative charging should not obscure whether each statutory element is independently proved.

Authorisation is especially important for education, cybersecurity research and responsible disclosure. Consent must come from a person entitled to permit the testing and must cover the relevant system, method, time and scope. A general educational purpose, the public availability of a system or weak security does not create authorisation. Exceeding an agreed testing boundary may change the legal assessment. Conversely, an accidental connection, passive observation or possession of a lawful tool should not be equated automatically with intentional intrusion. Context, logs, communications, persistence after warning, concealment, data use and attempts to obtain benefit are relevant to proving intent.

Participation in online groups also requires individualised proof. Membership, reputation or contact with offenders may be evidentially relevant, but it does not replace proof of contribution and intent. Liability as a co-author, organiser or helper depends on the role actually performed and the person's knowledge of the common conduct. This is important for young participants who may write code, provide credentials, host infrastructure or transfer funds without controlling the wider operation. Investigation should distinguish knowing assistance from negligence, coercion, grooming and exploitation.

4.4.3. Electronic evidence and procedural safeguards

The Criminal Procedure Code contains specific powers for electronic evidence. Article 191/a permits an order requiring the holder or controller to produce stored computer data and allows subscriber information to be requested from a service provider. In urgent circumstances, the prosecutor may issue a reasoned production order subject to judicial assessment within 48 hours. Article 208/a regulates seizure of computer data and systems, including access to connected data that are lawfully available from the system being searched, extraction of copies, restriction of access and preservation of integrity. Articles 299/a and 299/b provide for expedited preservation and partial disclosure of computer and traffic data. Articles 221–223 regulate interception and its authorisation (Republic of Albania, 1995, as amended).

Digital evidence is volatile, replicable and often mixed with large quantities of private information. Lawful seizure of a device is not the same act as searching all of its contents. A defensible investigation should define

the device or account, offence, categories of data, relevant period and search criteria. It should create and verify forensic copies where appropriate, document every access and transformation, preserve metadata and integrity, and maintain a clear chain of custody. Overbroad extraction can undermine necessity, proportionality and the reliability of the evidence.

Constitutional safeguards remain applicable online. Articles 35 and 36 protect personal data and the secrecy of communications, while Article 37 protects the home. Under Article 17, restrictions on rights must have a legal basis, pursue a legitimate public interest or protect the rights of others, remain proportionate and respect the essence of the right. Law No. 124/2024 on personal-data protection also regulates processing by competent authorities for the prevention, detection, investigation and prosecution of crime. Collection, retention, access, transfer and deletion of electronic evidence therefore require purpose limitation, security, accountability and effective remedies, alongside the procedural powers of the Criminal Procedure Code (Republic of Albania, 1998; Republic of Albania, 2024b).

4.4.4. Children and young adults

The study distinguishes minors aged 14–17 from young adults aged 18–24. The latter are generally processed under the ordinary adult system. Minors fall within the specialised framework of Law No. 37/2017, which gives priority to the best interests of the child, dignity, proportionality, education, rehabilitation and reintegration. Age and developmental capacity do not erase responsibility, but they affect participation rights, assessment, legal assistance, confidentiality, the choice of measure and the weight given to diversion. Children below the applicable age of criminal responsibility cannot be treated as criminally liable and require protection-oriented responses.

A cyber case involving a minor requires an individual assessment of conduct, harm, intent, technical role, maturity, peer influence, coercion, victimisation, family and school context, and prospects for desistance. Diversion is not impunity. It is a structured response that may combine acknowledgement of responsibility, repair, supervision, ethical technical education and restrictions tailored to the method of offending. Detention must remain a last resort and for the shortest appropriate period. Serious, repeated or organised conduct may justify formal prosecution, but even then the response should preserve realistic routes to education and lawful technical development (Republic of Albania, 2017; United Nations, 1989).

The victim–offender overlap is legally significant. A minor may be recruited to lend an account, move funds, test credentials or maintain infrastructure while also being threatened, deceived or exploited. Authorities should determine who initiated the relationship, controlled the proceeds, supplied instructions and could terminate participation. Safeguarding does not prevent investigation; it improves attribution by separating higher-level organisers from recruited or coerced participants.

4.4.5. Cybersecurity regulation and institutional responsibility

Law No. 25/2024 on Cybersecurity is primarily preventive and regulatory. It defines the national authority, CSIRT structures, risk-management measures, incident-reporting duties and obligations for operators of critical and important information infrastructures. Its administrative offences and sanctions do not automatically establish a Criminal Code offence. The two regimes may interact because weak controls create opportunity, incident reports may trigger investigation and preserved technical records may become evidence. Their legal bases, standards of proof and institutional purposes must nevertheless remain distinct (Republic of Albania, 2024a).

4.4.6. Cross-border cooperation

Subscriber information, traffic data, content and infrastructure are often held in different jurisdictions. The Budapest Convention provides a framework for preservation, mutual assistance and cooperation concerning

cybercrime and electronic evidence. Albania signed the Second Additional Protocol in 2023 and has worked with the Council of Europe on legislative alignment and implementation. The Protocol can improve direct cooperation and disclosure mechanisms, but speed cannot displace legality, necessity, proportionality, data protection, judicial control or an effective opportunity to challenge the use of evidence (Council of Europe, 2001; 2024; 2025).

The central legal conclusion is therefore bounded. Albania has substantive offences and procedural powers capable of addressing cyber-dependent conduct. The principal problems lie in precise classification, individual attribution, rights-compliant acquisition of electronic evidence, cross-border execution and the developmentally appropriate treatment of minors. Legal reform should be evaluated through the quality and lawfulness of decisions, not only through the number of proceedings or requests.

5. Digital communities and pathways into offending

5.1. Entry through curiosity and boundary testing

A common pathway begins with curiosity rather than a settled intention to cause harm. The young person learns basic coding, game modification or network concepts, tests passwords or tools, and receives approval for crossing a boundary. The first act may produce little visible harm, but it teaches three lessons: access is possible, detection is not immediate and peers value the result. In social-learning terms, imitation supplies the initial script and reinforcement changes the expected balance of rewards and costs.

The preventive window is early. Schools and universities should state clear rules about authorisation, logging, disclosure and responsible testing while also providing lawful environments in which technical curiosity is rewarded. Capture-the-flag exercises, supervised laboratories, vulnerability-disclosure education and ethical competitions can preserve challenge and status without a real victim. A warning detached from an alternative community is less likely to compete with a group that offers immediate feedback and belonging.

5.2. Progression through services, markets and specialisation

Progression becomes more serious when tools and skills are monetised. Online markets can divide labour among developers, access brokers, fraud operators, infrastructure providers and money mules. A young participant may initially understand only one task. Specialisation lowers the knowledge required for each actor and creates moral distance from the final victim. Reputation systems and repeated transactions reinforce reliability as a criminal identity.

Europol's assessments describe cybercrime as an increasingly professional ecosystem and warn that online platforms and encrypted communications can be used to recruit young people. The mechanism is not unique to cyber-dependent crime: social media can also recruit youth for fraud, violence or other organised activity (Europol, 2024a; 2024b). In Albania, the appropriate inference is a risk proposition, not a prevalence claim. Cross-border language networks, diaspora connections and widespread mobile access can make external communities locally accessible, but case-level and survey evidence is required before asserting their scale.

5.3. Victim–offender overlap and coercion

Young people may be victims and offenders within the same sequence. A person can be groomed, threatened with disclosure, induced to lend an account, or asked to move funds before understanding the wider scheme. Victimisation can also produce retaliatory offending or entry into peer groups that promise protection. A purely offender-centred assessment may miss coercion, exploitation and developmental vulnerability.

Assessment should therefore examine who initiated contact, whether threats or debt were used, who controlled accounts and proceeds, and whether the young person could exit safely. Safeguarding and

investigation are complementary: identifying exploitation can reveal higher-level organisers while allowing a proportionate response to the recruited youth.

6. Comparative European evidence and transferability

Comparative evidence is used functionally rather than to rank countries or import prevalence estimates. The relevant question is whether a foreign measure addresses a mechanism also plausible in Albania and whether institutional safeguards can be reproduced. Three models are especially relevant: empirical identification of pathways, targeted diversion after boundary crossing and preventive digital-citizenship education.

6.1. Evidence on pathways

A Dutch population study of 1,240 young people examined password guessing, denial-of-service attacks, technically assisted hacking and website defacement. More serious cyber-dependent conduct was embedded in social-learning environments and technical capability, while simpler conduct showed a different risk structure (Bekkers, Holt and Leukfeldt, 2026). Earlier youth research likewise found that deviant peer association contributed to cyber-deviance beyond low self-control (Holt, Bossler and May, 2012). These findings support differentiated measures, but their effect sizes cannot be transferred to Albania.

6.2. Diversion and lawful skill redirection

The Netherlands uses Hack_Right as an intervention after a cyber offence, including for young first-time offenders, with the aim of preventing escalation and redirecting technical ability. The broader Dutch prevention model also includes re_B00TCMP and educational initiatives developed with police, prosecution, probation, child-protection and private partners. The United Kingdom's Cyber Choices programme similarly combines legal awareness, victim understanding, early referral and pathways into lawful technical careers. These programmes illustrate functional substitution: prevention offers challenge, recognition and belonging rather than relying only on deterrent messages (Netherlands Police, 2026; National Crime Agency, 2026).

6.3. Digital citizenship and school prevention

Council of Europe digital-citizenship education promotes critical thinking, ethical awareness, rights and responsibility across formal and non-formal learning. Europol's Cyber Defenders resources use scenario-based learning to connect online safety, fraud, identity theft and grooming with real-world consequences. These models support practical education before offending occurs. Their transfer to Albania would require Albanian-language materials, teacher preparation, referral protocols and separation between safeguarding, school discipline and criminal reporting (Council of Europe, 2019; Europol, 2025).

6.4. Conditions for transfer to Albania

Albania shares high mobile connectivity, cross-border platforms and the need for electronic evidence, but differs in institutional capacity, educational provision, language networks and available data. Any pilot should define eligibility, legal authority, safeguarding, data processing, supervision and exclusion criteria. Outcomes should be pre-registered and should measure behaviour, repeat contact, victimisation, ethical reasoning, school attachment and lawful use of technical skills. Attendance alone is not evidence of effectiveness.

7. Integrated analytical model

The combined framework can be organised around five stages. First, digital exposure connects a young person with people, narratives, tools and targets. Second, definitions recast unauthorised conduct as harmless, deserved or prestigious. Third, capability develops through observation, practice and feedback. Fourth, opportunity supplies an accessible target with inadequate guardianship. Fifth, reinforcement determines whether

the conduct stops, repeats or becomes specialised. Movement is neither linear nor inevitable; intervention can redirect the pathway at every stage.

Table 1

Integrated model of youth cyber-offending and prevention

Stage	Digital manifestation	Criminological function	Preventive response
Exposure	Gaming groups, social media, messaging channels, forums, repositories and peer networks	Contact with models, narratives, tools and potential targets	Digital literacy; credible outreach; moderated communities; early referral
Definition	Unauthorised access framed as play, protest, intelligence or victimless conduct	Neutralisation lowers legal and moral inhibition	Scenario-based cyber ethics; victim-impact education; clear authorisation rules
Capability	Tutorials, scripts, practice, feedback and specialised division of labour	Technical skill makes conduct executable	Supervised labs; ethical competitions; mentoring; responsible disclosure
Opportunity	Weak credentials, exposed services, reusable data, low-friction payment or identity systems	Suitable target meets insufficient guardianship	Secure design; MFA; reporting; school, family and provider guardianship
Reinforcement	Status, access, money, belonging, excitement or avoidance of detection	Repetition, escalation and criminal identity consolidation	Lawful recognition and employment; proportionate intervention; protected exit

Source: Author's analytical synthesis.

Table 2

Recorded cybercrime proceedings in Albania 2024 and 2025

Indicator	2024	2025	Interpretive limit
Registered proceedings	303	206	Cases are not persons or prevalence
Proceedings sent to trial	19	17	May concern incidents registered earlier
Registered defendants	16	29	No published age cross-tabulation
Defendants sent to trial	59	24	Procedural timing affects annual totals
Convicted defendants	11	22	Conviction year may differ from registration year

Source: General Prosecutor of Albania, Annual Report on the State of Crime 2025, Table 35.

8. Critical assessment

Social learning has strong explanatory value where cyber-offending involves sustained interaction, shared rationalisations, technical instruction and reputation. It explains how a community can turn isolated experimentation into a stable role and how lawful mentors, employment and peer groups may support desistance. It does not, however, establish that these mechanisms operate with the same strength in Albania.

Social learning cannot stand alone. Self-control may matter for opportunistic misuse; strain may shape motives; routine activity explains accessible targets; and perceived risk affects decision-making (Gottfredson and Hirschi, 1990). Different mechanisms may dominate at different stages and for different offences. The four

propositions in this article are therefore theoretically derived hypotheses for future testing, not empirical findings about Albanian youth.

The principal Albanian evidential problem is underdetermination. Connectivity, technical ability and recorded cybercrime may coexist without a causal relationship. Administrative categories omit undetected conduct and may change with reporting, classification and institutional practice. International research makes the proposed mechanisms plausible and Albanian conditions make them policy-relevant, but national data are required to estimate prevalence, direction and relative strength.

Prevention may also cause harm. Poorly supervised groups can reward deviant stories, exchange operational knowledge and create new networks (Dishion, McCord and Poulin, 1999). Pilot programmes must control technical detail, structure peer roles, protect victims and offer credible lawful status. Their effects must be evaluated rather than assumed.

9. Implications for prevention and criminal justice

9.1. Build an Albanian evidence base

Albania should establish and publish age-disaggregated cybercrime indicators covering suspects, defendants, outcomes, diversion and repeat contact, while avoiding disclosure risks. Police and prosecution forms should capture recruitment, online-community involvement, technical role, coercion and financial motivation. A national youth cyber-behaviour survey, administered with strong ethical protections, would measure both offending and victimisation and permit testing of social-learning and opportunity variables.

9.2. A national research design

A first national study should use an anonymous stratified survey of secondary-school pupils, vocational students and university students aged 14–24, combined with a smaller justice-involved sample. The questionnaire should distinguish attempted and completed behaviours, authorisation, frequency, harm, financial gain, peer conduct, online-group participation, favourable definitions, neutralisations, technical capability, guardianship, victimisation and willingness to desist. Separate consent and safeguarding procedures are required for minors, and operational details that could facilitate offending should not be collected unnecessarily.

A longitudinal design with at least two measurement waves would improve causal inference. It could test whether peer association precedes behaviour, whether young people select similar peers after offending, and whether lawful mentoring changes reinforcement over time. Administrative linkage should use pseudonymised identifiers and independent governance. Interviews with investigators, prosecutors, educators, cybersecurity mentors and young participants could then explain patterns that survey coefficients alone cannot capture.

Evaluation should be built into every pilot. Primary outcomes might include self-reported harmful behaviour, repeat justice contact and verified completion of responsible technical activities. Intermediate outcomes should include changes in favourable definitions, peer networks, school attachment, ethical reasoning, victim awareness and legitimate employment or training. A programme should not be declared successful merely because participants attended or because recorded incidents fell during a period of changing detection.

9.3. Teach cyber ethics through practice

Cybersecurity education should move beyond password hygiene. Students need concrete instruction on authorisation, privacy, electronic evidence, responsible disclosure, criminal liability and victim impact. Scenario-based exercises can expose neutralisations and require students to distinguish observation, testing and intrusion. Teachers require referral pathways when conduct exceeds school discipline but does not yet justify a purely punitive response.

9.4. Create lawful status and skill pathways

A theoretically supported prevention principle requiring national evaluation is functional substitution. If an online group provides challenge, reputation, belonging and income, an awareness poster supplies none of those functions. Universities, AKSK, technology firms and civil society should pilot and evaluate supervised laboratories, competitions, apprenticeships, mentoring and entry routes into cybersecurity employment. The National Cybersecurity Center of Excellence envisaged in the 2025–2030 Strategy offers an institutional anchor for talent identification and ethical formation, provided access extends beyond already privileged students.

Participation criteria should not stigmatise young people solely because they have offended. Carefully governed second-chance pathways can support desistance, but access to sensitive systems must be based on individual risk assessment, supervision and legal safeguards. Success should be measured through education, employment, reduced harmful behaviour and sustained pro-social engagement, not attendance alone.

9.5. Strengthen families, schools and platform guardianship

Parents do not need to become forensic specialists. However, they should recognise warning signs and know how to respond. Such signs include unexplained income, repeated account changes, coercive online relationships and extreme secrecy. Other signs are persistent night-time activity, withdrawal from school or claims of being trapped by a group. None is proof of crime. The objective is early conversation and confidential support. Schools should combine technical monitoring with trust, because surveillance without legitimacy can displace conduct to less visible spaces.

Platforms and service providers should reduce discoverability of criminal recruitment, preserve evidence lawfully, provide usable reporting channels and cooperate across borders. Guardianship should be layered: secure system design, multi-factor authentication, rapid account recovery, user education, family support, school protocols and specialised investigation each close a different opportunity.

9.6. Use proportionate, developmentally informed responses

Diversion is appropriate where responsibility can be acknowledged, harm repaired and risk safely managed. Conditions may include supervised education, restrictions tailored to the method of offending, restorative components where suitable, and mentoring. Serious, repeated or organised offending may require prosecution, but sentencing should still address criminogenic needs and preserve realistic routes to lawful technical identity.

International cooperation is indispensable because data, infrastructure, victims and offenders may be distributed across jurisdictions. Effective use of Budapest Convention channels and the Second Additional Protocol must be paired with procedural safeguards, privacy protection and judicial oversight. Speed cannot displace legality; otherwise enforcement undermines the trust required for reporting and cooperation.

10. Conclusion

This article develops a theoretical, doctrinal and policy model for youth cyber-offending in Albania. It does not claim to measure prevalence or prove causal pathways among Albanian young people. Its contribution is to connect social learning, criminal opportunity and the national legal framework and to identify propositions that can be tested with Albanian data.

The first research question concerns digital communities. The analysis shows that peers and online groups can transmit knowledge, favourable definitions, neutralisations and rewards. These mechanisms may support initiation, repetition and desistance, but their Albanian prevalence remains unknown. The second question concerns opportunity. Accessible targets, weak guardianship and usable capability can convert learned attitudes into conduct. Neither connectivity nor technical skill alone establishes criminal propensity.

The third question asks what Albanian evidence can establish. Official statistics confirm that cybercrime proceedings and juvenile cases enter the criminal-justice system, but the datasets are not linked by age, offence, role, motivation, digital community or outcome. The resulting data gap is an institutional finding, not evidence of a specific youth-cybercrime rate. It prevents causal inference and limits evaluation of diversion and prevention.

The legal analysis confirms that liability must remain offence-specific and individualised. Albanian law criminalises unauthorised access, unlawful interception, interference with data and systems, misuse of devices, computer fraud and computer forgery. Investigators must distinguish authorised testing from intrusion, lawful tools from criminal use, and group association from knowing participation. Electronic evidence must be obtained with judicial control, integrity safeguards, proportionality and data protection. For minors, specialisation, best interests, diversion, rehabilitation and reintegration remain central.

The fourth question concerns response. Albania should combine age-disaggregated data, behaviour-specific research, practical cyber-ethics education, lawful technical pathways, family and school referral, secure system design and proportionate justice. Dutch and British diversion models and Council of Europe digital-citizenship education offer functions that can be adapted, but not copied without local legal authority, safeguarding and evaluation.

Future research should test the four propositions with separate measures for unauthorised access, disruption, malware, fraud and account facilitation. Longitudinal surveys, qualitative interviews and pseudonymised administrative linkage can clarify whether peers precede offending, whether young people select similar peers and whether lawful mentoring changes reinforcement. Programme success should be judged by behaviour, repeat contact, victim outcomes, education and lawful technical engagement, not attendance or short-term changes in recorded incidents.

The broader conclusion is that cybersecurity and youth development are compatible goals. Strong guardianship can reduce opportunity, ethical communities can redirect learning and proportionate justice can prevent harm without closing lawful futures. Technical competence is a public asset. Its social value depends on the legal, educational and social environment in which it is learned, recognised and used.

References

AKERS, R. L. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press, 1998.

BANDURA, A. *Social Learning Theory*. Englewood Cliffs, NJ: Prentice Hall, 1977.

BEKKERS, L. M. J.; HOLT, T. J.; LEUKFELDT, E. R. The Psychological Correlates of Cybercrime Offending: Exploring the Self-Control/Social Learning Relationship in Serious Cyber-Dependent Crime. *European Journal of Criminology*, 2026, vol. 23, no. 4, pp. 610–637. DOI: 10.1177/14773708251378356.

BURGESS, R. L.; AKERS, R. L. A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*, 1966, vol. 14, no. 2, pp. 128–147. DOI: 10.2307/798612.

COHEN, L. E.; FELSON, M. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 1979, vol. 44, no. 4, pp. 588–608. DOI: 10.2307/2094589.

COUNCIL OF EUROPE. *Albania Commences Legislative Reform for the Ratification and Effective Implementation of the Second Additional Protocol to the Budapest Convention*. Strasbourg, 13 November 2024.

COUNCIL OF EUROPE. *Convention on Cybercrime*, ETS No. 185. Budapest, 23 November 2001.

COUNCIL OF EUROPE. *CyberSEE Continues to Support Albania in Aligning Its Legislation with the Second Additional Protocol to the Convention on Cybercrime*. Strasbourg, 28 May 2025.

COUNCIL OF EUROPE. Recommendation CM/Rec(2019)10 of the Committee of Ministers to Member States on Developing and Promoting Digital Citizenship Education. Strasbourg, 21 November 2019.

COUNCIL OF MINISTERS OF ALBANIA. National Cybersecurity Strategy 2025–2030. Tirana, 2025.

DISHION, T. J.; MCCORD, J.; POULIN, F. When Interventions Harm: Peer Groups and Problem Behavior. *American Psychologist*, 1999, vol. 54, no. 9, pp. 755–764. DOI: 10.1037/0003-066X.54.9.755.

EUROPEAN COMMISSION. Albania Report 2025. SWD(2025) 750 final. Brussels, 4 November 2025.

EUROPEAN PARLIAMENT AND COUNCIL. Directive 2013/40/EU of 12 August 2013 on Attacks against Information Systems. *Official Journal of the European Union*, L 218, 14 August 2013, pp. 8–14.

EUROPOL. Cyber Defenders: Raising Awareness for Cybercrime via Roblox. The Hague: Europol, 2025.

EUROPOL. Internet Organised Crime Threat Assessment 2024. The Hague: Europol, 2024a.

EUROPOL. The Recruitment of Young Perpetrators for Criminal Networks. The Hague: Europol, 2024b.

EUROPOL. Youth Pathways into Cybercrime. The Hague: European Cybercrime Centre, 2017.

GENERAL PROSECUTOR OF ALBANIA. Annual Report on the State of Crime for 2025. Tirana: Office of the General Prosecutor, April 2026, especially pp. 147–149, 170–171 and Table 35.

GOTTFREDSON, M. R.; HIRSCHI, T. A General Theory of Crime. Stanford: Stanford University Press, 1990.

HOLT, T. J.; BOSSLER, A. M.; MAY, D. C. Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, 2012, vol. 37, no. 3, pp. 378–395. DOI: 10.1007/s12103-011-9117-3.

HOLT, T. J.; BURRUSS, G. W.; BOSSLER, A. M. Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, 2010, vol. 33, no. 2, pp. 31–61. DOI: 10.1080/0735648X.2010.9721287.

INSTAT. Crime and Criminal Justice Statistics 2025. Tirana: Institute of Statistics, 27 April 2026.

INSTAT. Survey on Information and Communication Technology Usage in Households and by Individuals in 2025. Tirana: Institute of Statistics, 11 December 2025.

NATIONAL CRIME AGENCY. Cyber Choices. London: National Crime Agency, 2026.

NETHERLANDS POLICE. What Is Cyber Offender Prevention? The Hague: Politie, 2026.

PRATT, T. C.; CULLEN, F. T.; SELLERS, C. S.; et al. The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly*, 2010, vol. 27, no. 6, pp. 765–802. DOI: 10.1080/07418820903379610.

REPUBLIC OF ALBANIA. Constitution of the Republic of Albania, 1998, as amended.

REPUBLIC OF ALBANIA. Criminal Code, Law No. 7895 of 27 January 1995, as amended.

REPUBLIC OF ALBANIA. Criminal Procedure Code, Law No. 7905 of 21 March 1995, as amended.

REPUBLIC OF ALBANIA. Law No. 124/2024 of 19 December 2024 on Personal Data Protection, 2024b.

REPUBLIC OF ALBANIA. Law No. 25/2024 of 21 March 2024 on Cybersecurity. *Official Gazette* No. 67, 2024a.

REPUBLIC OF ALBANIA. Law No. 37/2017 of 30 March 2017, Code of Criminal Justice for Children, as amended.

SNYDER, H. Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 2019, vol. 104, pp. 333–339. DOI: 10.1016/j.jbusres.2019.07.039.

SUTHERLAND, E. H. *Principles of Criminology*. 4th ed. Philadelphia: J. B. Lippincott, 1947.

SYKES, G. M.; MATZA, D. Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 1957, vol. 22, no. 6, pp. 664–670. DOI: 10.2307/2089195.

UNITED NATIONS. Convention on the Rights of the Child. Adopted 20 November 1989, entered into force 2 September 1990, 1577 UNTS 3.

ZHOU, Y. Traditional Social Learning Predicts Cyber Deviance? Exploring the Offending Versatility Thesis in Social Learning Theory. *Behavioral Sciences & the Law*, 2024, vol. 42, no. 4, pp. 417–434. DOI: 10.1002/bsl.2664.