THE ECONOMICS OF DIGITAL CRIME: UNDERSTANDING THE CYBERCRIME VALUE CHAIN

CZU: 343.9:007.52+004.056
DOI: https://doi.org/10.53486/tids2026.32

DAVID NAVAS
Financial University under the Government of the Russian Federation
e-mail: d.navvas@gmail.com
ORCID ID: 0009-0008-7333-5991

IVAN KULAKOV
Financial University under the Government of the Russian Federation
e-mail: kulakovi849@gmail.com
ORCID ID: 0009-0007-8824-9239

DINARA ORLOVA
DSC, Professor, Department of Economics
Financial University under the Government of the Russian Federation
e-mail: DROrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

Abstract. Cybercrime has developed into a global market in which different participants supply distinct services rather than carrying out every stage of an attack themselves. The resulting division of labour links malware developers, access sellers, platform operators and financial intermediaries in arrangements that resemble commercial supply chains. This article considers the economic implications of that shift, focusing on how specialization, digital platforms and technological change shape the organization and durability of illicit online markets.

The discussion draws on Transaction Cost Economics, Platform Economy Theory and Value Chain Theory to examine how these markets are organized. It considers Initial Access Brokers, Ransomware-as-a-Service arrangements, darknet marketplaces, cryptocurrency-related laundering services and the growing use of artificial intelligence. Particular emphasis is placed on the business arrangements behind these activities: affiliate relationships, outsourced tasks, specialized suppliers and platforms that can serve many participants at once.

Evidence from cybersecurity reports, threat intelligence publications and law-enforcement assessments points to a recurring economic problem: some cybercriminal operations can be initiated at a modest cost while exposing victims to much larger losses. Marketplaces also help otherwise anonymous buyers and sellers locate one another, assess counterparties and arrange transactions. AI tools may reduce the time and expertise needed for certain tasks, although their effects differ across activities and are not always straightforward to measure.

The analysis therefore treats cybercrime as more than a collection of technical incidents. It is also a cross-border system of incentives, exchanges and specialized services. This perspective suggests that technical defenses are necessary but insufficient on their own: interventions must also address the markets, intermediaries and financial incentives that allow criminal operations to continue.

Keywords: Cybercrime economy, cybercrime value chain, ransomware-as-a-service, darknet platforms, digital crime monetization, artificial intelligence in cybercrime.

JEL Classification: K42, O33, L86

INTRODUCTION

The organization of cybercrime has changed considerably over the last twenty years. An attack that once might have depended on one individual carrying out several tasks can now involve separate providers of software, infrastructure, stolen access and payment services. These participants need not belong to a single organization; they may cooperate only for a particular transaction. In this respect, parts of the underground economy have begun to resemble legitimate digital industries, with recognizable divisions of labour, intermediaries and methods of generating revenue. Such arrangements make it easier to repeat operations and replace individual participants when necessary.

As economic activity has moved online, the possible consequences of cybercrime have grown with it. Cybersecurity Ventures (2025) projects annual worldwide cybercrime damages above USD 10.5 trillion, although estimates of this kind should be read as projections rather than observed criminal revenue. Businesses now rely heavily on cloud services, remote access, electronic payments and digitally connected suppliers. Each dependency can create an additional point of exposure. The resulting risks are not confined to technology companies: public authorities, banks, hospitals, multinational businesses and operators of essential infrastructure all depend on systems that can be disrupted or misused.

Greater spending on cybersecurity and closer cooperation between enforcement agencies have not removed the incentives behind cybercrime. An important reason is the gap between what an attacker may need to spend and what a successful incident can cost the victim. Certain phishing or credential-theft operations require limited infrastructure, while the consequences can include business interruption, remediation expenses and direct financial loss. Not every attempt succeeds, and criminal revenue is not the same as victim damage. Nevertheless, the possibility of substantial returns from comparatively inexpensive operations helps explain why new participants continue to enter these markets.

Crime-as-a-Service (CaaS) has made this division of labour especially visible. Ransomware-as-a-Service (RaaS), Malware-as-a-Service (MaaS) and phishing-as-a-service arrangements allow one participant to use tools or infrastructure supplied by another. A buyer may therefore avoid developing software, maintaining servers or acquiring every relevant skill independently. Darknet marketplaces and encrypted channels provide venues where these services can be advertised and negotiated. The practical consequence is a lower entry threshold for some criminal activities and a market in which specialized suppliers can serve multiple customers.

These exchanges face a problem familiar to economists: participants often know little about the people on the other side of a transaction. Darknet marketplaces respond with mechanisms that also appear in lawful online commerce, including seller ratings, escrow arrangements, dispute procedures and verification systems. None of these features eliminates fraud or guarantees trust. They can, however, make transactions more predictable and reduce the effort involved in finding a counterparty. Where a platform attracts enough buyers and sellers, its growing network may encourage additional specialization and trading activity.

Artificial intelligence adds another layer to these developments. Generative tools can assist with drafting persuasive messages in several languages, adapting social-engineering material and automating parts of an operation. Deepfake audio and video also create opportunities for impersonation. The economic significance lies partly in the time and skill required to perform these tasks: where automation works reliably, it may lower the marginal cost of repeating them. The extent of that advantage depends on the type of attack, however, and should not be assumed to be identical across all criminal activities.

This article examines the relationships connecting participants in the cybercrime value chain and asks why these arrangements can persist despite defensive and enforcement efforts. Transaction Cost Economics helps explain exchanges between unfamiliar actors; Platform Economy Theory sheds light on the role of marketplaces and network effects; and Value Chain Theory clarifies the separation of tasks. The discussion concentrates on access brokers, ransomware operations, darknet trading venues, cryptocurrency-related financial services and the use of AI in criminal workflows.

The analysis is based on published cybersecurity assessments, threat intelligence research, law-enforcement material and established economic literature. These sources do not provide a complete picture of hidden markets, and estimates of costs, proceeds and losses are not always directly comparable. Even with those limitations, they reveal organizational patterns that cannot be explained solely by software vulnerabilities. The central argument is that the structure of criminal markets matters: technical controls may stop particular attacks, while changes to incentives and intermediary services may affect the conditions under which new attacks are organized.

THE CYBERCRIME VALUE CHAIN

A defining feature of contemporary cybercrime is that its participants can divide an operation into separate, tradable tasks. The person who obtains access to a company network may never deploy the ransomware used against it, and the developer of that ransomware may have no direct contact with the victim. These relationships create a loose production network rather than a single, self-contained group. Specialization can improve the quality of particular services and allow operations to expand without every participant acquiring the same expertise. It can also make the wider market difficult to disrupt by targeting one actor.

Porter (1985) introduced the value-chain framework to describe how interconnected activities contribute to the production of economic value. Applied to cybercrime, the framework draws attention to the sequence of services needed to turn a technical opportunity into illicit proceeds. Infrastructure, unauthorized access, exploitation, monetization and movement of funds may be handled by different suppliers. This is not to suggest that criminal and lawful production are equivalent, but the comparison helps identify where participants specialize, exchange services and shift costs or risks onto others.

An operation commonly begins with tools and infrastructure. Developers and service providers may supply malicious software, phishing kits, credential-stealing programs, exploit tools or hosting arrangements that other actors subsequently use. Rather than selling every product outright, some suppliers rely on subscriptions or a share of the proceeds. Ransomware-as-a-Service (RaaS) illustrates the arrangement: one group maintains the software and supporting infrastructure, while affiliates select victims and conduct attacks. Payments are then divided according to the parties' agreement. Malware-as-a-Service (MaaS) follows a related logic. By separating development from deployment, these models allow participants with different skills and resources to cooperate without forming a conventional organization.

Unauthorized access to an organization's systems has itself become a product. Initial Access Brokers (IABs) focus on obtaining and selling that access rather than necessarily using it for extortion or fraud. Their customers may be other criminal actors seeking an entry point for a later operation. Listings can circulate through darknet marketplaces or encrypted channels, with the value of an offer shaped by the target and the privileges available. Access can originate in phishing, exploited VPN weaknesses, credential stuffing, malware infections, attempts against Remote Desktop Protocol

(RDP) services or assistance from insiders. The broker's role separates the acquisition of access from the decisions made after a compromise.

The existence of a market for initial access shows how even an early stage of an attack can be priced and traded. Threat intelligence reports describe offers ranging from several hundred dollars to tens of thousands, depending on the organization's characteristics and the level of control provided. These figures should be understood as reported market observations, not a uniform price schedule. A buyer who already has the required tools can purchase access instead of spending time obtaining it. Meanwhile, a seller can specialize in finding entry points without taking on every risk associated with the subsequent attack.

Remote access services are important in this market because organizations use them to support ordinary work. RDP and VPN connections became particularly significant as remote working arrangements expanded. Their usefulness also creates opportunities when credentials are stolen, authentication is weak or exposed services are inadequately secured. Criminal actors may search for reachable RDP systems and attempt to enter using compromised credentials or password-guessing techniques. A valid VPN account can likewise provide a route into an internal environment. In both cases, the economic value of access comes from the fact that it can be transferred to another participant for further exploitation.

Phishing and social engineering remain attractive methods of obtaining credentials because a single campaign can reach many potential victims. Messages may appear to come from banks, software vendors, IT staff or senior managers, and their purpose is to persuade recipients to disclose information or open harmful material. AI tools can make such messages easier to draft, translate and tailor to particular contexts. That capability may reduce preparation time and help attackers operate across languages. Whether it increases success rates in a given campaign is an empirical question, but it clearly changes the resources needed to produce plausible-looking fraudulent communications.

Once access has been obtained, the next participants may investigate the compromised environment, seek higher privileges, maintain their foothold, extract information or install ransomware. Extortion has also become more varied. In a so-called double-extortion incident, attackers combine encryption with threats to disclose stolen data. Triple-extortion schemes may add pressure on customers, partners or other parties connected to the victim. These tactics matter economically because they create several possible sources of leverage over the same organization, even when the technical stages of an attack are carried out by different people.

The monetization stage turns access, information or disruption into a possible source of income. Payments may come from ransomware demands, financial fraud, stolen assets or the resale of data. Underground markets list different kinds of information, including medical records, payment details, wallet credentials and complete identity profiles sometimes called 'fullz'. Their prices vary because not all stolen data are equally useful or easy to exploit. Factors such as freshness, completeness, scarcity and the effort required to use the information can affect what a buyer is willing to pay. A listing price, however, should not be confused with a completed sale or realized profit.

Darknet marketplaces provide a meeting point for suppliers and customers who might otherwise struggle to locate one another. They may host offers involving malicious software, compromised accounts, access services and ways to move illicit funds. Because the parties are often anonymous, uncertainty about delivery and payment is especially pronounced. Escrow, seller histories, reviews and dispute procedures attempt to address that uncertainty, although manipulation and outright fraud remain possible. The comparison with legitimate digital platforms is therefore organizational rather

than moral: both types of intermediary can lower search and coordination costs by bringing separate sides of a market together.

After obtaining proceeds, criminal actors may seek to move or convert them in ways that complicate investigation. Reported methods include cryptocurrency mixers, decentralized exchanges, peer-to-peer transfers and privacy-oriented assets such as Monero. Some services perform these functions for other participants and charge a fee. This creates another area of specialization within the wider market. It is important, however, not to treat every use of a privacy technology or decentralized financial service as criminal; the relevant issue here is the use of such arrangements to handle proceeds of illegal activity.

Seen as a whole, the value chain reveals a market held together by transactions between specialists. Developers, brokers, affiliates, marketplace operators and financial intermediaries can exchange services without taking responsibility for an entire operation. This arrangement resembles outsourcing in lawful industries, even though its purpose and consequences are fundamentally different. It helps explain how criminal activity can continue across borders and why the disruption of one supplier may leave other parts of the market functioning. The resulting damage can be substantial even when individual stages are comparatively inexpensive.

ECONOMICS OF CYBERCRIME

The economic importance of cybercrime has increased as firms, public institutions and households have become more dependent on connected technologies. Cloud services, remote access and digital payments support legitimate growth, but they also widen the range of systems that can be attacked or misused. Cybersecurity Ventures (2025) projects worldwide cybercrime damages exceeding USD 10.5 trillion per year. The estimate conveys the possible scale of the problem, although projected aggregate losses should not be read as a direct measure of money earned by criminals. Distinguishing these concepts is essential when examining incentives and profitability.

A useful starting point is the difference between the resources needed to attempt an attack and the losses a victim may suffer if it succeeds. Some forms of cybercrime can be repeated with relatively little additional expenditure once the tools and infrastructure are available. They can also be conducted across national borders without the same physical presence required in many traditional crimes. Yet low apparent entry costs do not mean every operation is profitable: unsuccessful attempts, purchased services, failed payments and enforcement risks also matter. The economic attraction lies in the possibility that a successful operation produces returns much larger than the initial outlay.

Ransomware operations illustrate how the organization of production affects costs. A developer may concentrate on maintaining software and infrastructure while affiliates carry out attacks against particular targets. Revenue-sharing agreements then allocate proceeds between those involved. The model resembles a franchise in its division of responsibilities, although relationships between participants may be unstable and subject to conflict. For a developer, recruiting affiliates can extend reach without managing each incident directly. For an affiliate, using an existing service may be less demanding than building the required tools independently. These incentives help explain the persistence of ransomware markets.

The gap between attack expenditure and victim damage is particularly visible when an incident interrupts business operations. A criminal actor might purchase credentials, a phishing kit or access to a network at a comparatively modest price. The affected organization, by contrast, may face downtime, investigation expenses, lost business, reputational harm and regulatory consequences, in

addition to any direct payment or theft. Those losses cannot automatically be counted as the attacker's revenue or return on investment (ROI). They do, however, show how a small expenditure on one side of a transaction can impose much larger costs on the other.

Figure 1 compares estimated attack costs with potential financial damage across several categories of cybercrime. It is intended to illustrate the scale of possible differences rather than to provide a direct calculation of criminal profits.



Figure 1. Relationship Between Average Attack Costs and Potential Financial Damage in Cybercrime Operations.

Source: *Developed by the author based on data from Cybersecurity Ventures (2025), IBM (2024), Coveware(2024), Microsoft (2024), and Chainalysis (2025).*

Figure 1 highlights the potential disparity between the resources associated with an attack and the damage that may follow. Phishing and credential theft appear at the lower-cost end of the comparison, while ransomware and supply-chain incidents may be associated with much larger losses. These categories are not directly interchangeable, and the plotted figures should not be interpreted as a consistent measure of expected returns. The comparison nevertheless helps explain the incentive problem: the expenditure required to initiate an incident may be small relative to the disruption imposed on an organization.

Markets for criminal services also change the economics of participation. A darknet platform can bring together people who sell access, software or other services and those who want to purchase them. Ratings, escrow, vendor verification and dispute procedures may reduce the time spent searching and negotiating, even where no legal contract can be enforced. This resembles the transaction-cost problem discussed by Coase (1937) and Williamson (1985). The platform does not eliminate uncertainty, but it can provide informal arrangements that make repeated exchanges possible between participants who would otherwise have difficulty trusting one another.

Network effects offer a further explanation for the attraction of established marketplaces. More buyers can encourage additional sellers to list specialized services; a broader range of sellers may, in turn, make the platform more useful to buyers. Access brokers, malware developers and financial

intermediaries may therefore concentrate where they expect to find demand. This feedback can support liquidity and specialization, although it also makes successful platforms visible to investigators and vulnerable to disruption. The market is thus shaped by competing pressures: the benefits of concentration and the risks that accompany it.

Artificial intelligence may influence this structure by changing how much time and expertise particular tasks require. Generative systems can help produce tailored phishing messages, translate fraudulent communications and imitate the style of trusted individuals. Synthetic voices and deepfake media create additional opportunities for deception in financial and social-engineering schemes. AI tools may also assist with coding or information gathering. These uses do not make sophisticated attacks effortless, but they can shift some work from specialist operators to widely available software, altering the division of labour within criminal markets.

From an economic perspective, the important question is whether these tools reduce the additional cost of repeating an operation. Where AI can reliably automate drafting, translation or routine preparation, the same actor may be able to produce more material in less time. Other stages still require judgment, access and technical knowledge. It is therefore more accurate to describe AI as a potential source of productivity gains than as a universal explanation for cybercrime growth. Its effect on participation and scale will depend on the tasks being automated and the defenses encountered.

The resilience of these markets creates difficulties for enforcement. Removing a prominent ransomware group or shutting down a marketplace can interrupt particular relationships and impose real costs on participants. Yet developers, affiliates and brokers may move to another venue or establish new identities when their tools and contacts remain available. The modular structure of the market makes substitution possible. This does not mean enforcement is ineffective; rather, it suggests that lasting disruption may require attention to the relationships and services that allow operations to be reassembled after an intervention.

Cybercrime is therefore sustained by more than the availability of vulnerable systems. Specialized suppliers, digital marketplaces, automation and ways to transfer proceeds affect the cost of participation and the likelihood that an operation can be organized. Their interaction can make criminal activity scalable even when particular actors disappear. An economic analysis complements technical cybersecurity by identifying the incentives and intermediary services behind attacks. Policies that change those incentives may be as important as measures that address individual vulnerabilities or incidents.

CONCLUSION

The evidence considered in this article points to a significant organizational change in cybercrime. Instead of relying exclusively on individuals who perform every task, many operations now draw on networks of specialized suppliers. Malware developers, Initial Access Brokers, ransomware affiliates, marketplace operators and financial intermediaries can contribute separate services to a common sequence of activities. This division of labour makes it easier to combine expertise and replace individual providers. It also means that understanding a single attack is not always enough to understand the market that made the attack possible.

The analysis also shows why concepts from platform economics are useful. Darknet marketplaces connect suppliers and buyers and may reduce search, bargaining and coordination costs through reviews, escrow and dispute procedures. Crime-as-a-Service models separate the production of tools from their use, enabling participants to purchase capabilities they do not possess themselves.

AI may extend this process by reducing the time needed for selected tasks. Together, these developments help explain the organizational flexibility of cybercrime without implying that every criminal operation follows the same model.

Enforcement faces the challenge of disrupting relationships rather than only individual offenders or pieces of infrastructure. When a platform closes, some participants may migrate; when a group is dismantled, affiliates may seek new partners. Such adaptation is possible because many services are transferable across organizations. This does not diminish the value of investigations, arrests or technical takedowns. It indicates that the broader effects of these actions should also be assessed in terms of market access, replacement costs and the ability of criminal participants to rebuild their networks.

Cybercrime should consequently be studied as both a security problem and an economic system. Technical vulnerabilities help explain how attacks occur, while specialization, transaction costs and incentives help explain why particular forms of criminal activity continue. A more effective response will combine defensive improvements with efforts to disrupt the services, financial channels and market arrangements that support repeated operations. Examining those underlying structures provides a clearer basis for evaluating which interventions are likely to produce lasting effects.

REFERENCES

Chainalysis, 2025. *The Chainalysis Crypto Crime Report*. Available at: https://www.chainalysis.com/ [Accessed 14 May 2026].

Coase, R.H., 1937. The nature of the firm. *Economica*, 4(16), pp. 386–405.

Coveware, 2024. *Quarterly Ransomware Reports*. Available at: https://www.coveware.com/blog [Accessed 12 May 2026].

CrowdStrike, 2025. *Global Threat Report 2025*. Available at: https://www.crowdstrike.com/global-threat-report/ [Accessed 14 May 2026].

Cyberint, 2025. *Initial Access Broker Report 2025*. Available at: https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf [Accessed 15 May 2026].

Cybersecurity Ventures, 2025. *Official Cybercrime Report 2025*. Available at: https://cybersecurityventures.com/official-cybercrime-report-2025/ [Accessed 15 May 2026].

Europol, 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Available at: https://cybilportal.org/publications/internet-organised-crime-threat-assessment-iocta-2024/ [Accessed 15 May 2026].

Group-IB, 2025. *High-Tech Crime Trends 2025*. Available at: https://www.group-ib.com/landing/high-tech-crime-trends-2025/ [Accessed 14 May 2026].

IBM Security, 2024. *Cost of a Data Breach Report 2024*. Available at: https://www.ibm.com/reports/data-breach [Accessed 12 May 2026].

Microsoft, 2024. *Microsoft Digital Defense Report 2024*. Available at: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024 [Accessed 12 May 2026].

Porter, M.E., 1985. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press.

Rochet, J.-C. and Tirole, J., 2003. Platform competition in two-sided markets. *Journal of the European Economic Association*, 1(4), pp. 990–1029.

Sophos, 2024. *The State of Ransomware 2024*. Available at: https://www.sophos.com/en-us/content/state-of-ransomware [Accessed 14 May 2026].

Williamson, O.E., 1985. *The Economic Institutions of Capitalism*. New York: Free Press.

Zscaler ThreatLabz, 2025. *AI phishing and cyber threat report*. Available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-ai-phishing [Accessed 15 May 2026].