Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215963

A comprehensive review of effective methods for counteracting cybercrime

Jakub SYTA
Morskie Centrum Cyberbezpieczeństwa
Akademia Marynarki Wojennej w Gdynii
ORCID: 0000-0002-0115-6432
E-mail: j.syta@amw.gdynia.pl

Abstract

The purpose of this article is to attempt to identify methods of counteracting cybercrime that would effectively discourage cybercriminals from continuing their activities and structure them in a form allowing to choose potential options available for law enforcement. This article aims to prove the thesis that a significant reduction in cybercrime is achievable; however, it requires undertaking radical legislative changes and adapting the legal system to the dynamically evolving threats in cyberspace. The inspiration for this article came from observations made during a research internship that the author undertook at one of a European police unit specializing in combating cybercrime.

Presented article is of a theoretical and analytical nature and is based on the application of methods appropriate to the social sciences, particularly the security sciences. The methodological objective was to examine possible means of effectively counteracting cybercrime, drawing on real-world incidents observed in various countries. The research was conducted on the basis of an analysis of secondary sources of knowledge, employing a qualitative approach.

Keywords

cybercrime, L0cate, law enforcement

Introduction

The phenomenon of cybercrime is escalating rapidly. Statistics published by the Interpol indicate that there has been a significant rise in reported cyber-attacks, highlighting the global reach and increasing sophistication of malicious actors[1]. Similarly, the FBI has reported a substantial surge in cyber-related incidents, with ransomware and phishing attacks posing considerable threats to

[1] INTERPOL (2025) Africa Cyberthreat Assessment Report – 4th edition. INTERPOL, Lyon. Available at: https://www.interpol.int/en/content/download/23094/file/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf [accessed: 24.10.2025].

both private and public sectors[2]. Statistics from the polish Central Bureau for Combating Cybercrime (CBZC) also clearly state that Polish cyber-police is fully engaged[3]. According to estimates every fifth crime performed in Poland already is cyber related[4]. However, the number of ongoing cases does not necessarily correspond to the number of convictions, and the rising statistics do not suggest that sentences are an effective deterrent.

Cybercrime started to be “annoying” due to its significant rise. Internet users fear to lose their money or freedom. Companies fear to lose money, reputation, business continuity or strategic advantage. Governments fear to lose the possibility to provide crucial services to their citizens and to leak secrets. A number of options can be identified to deal with this situation:

- accept current situation and do nothing
- wait for criminals to become honest citizens
- wait for internet users to be resilient to any cyberattacks
- monitor every internet activity, identify all internet users
- change the way cybercriminals are being caught and prosecuted

The purpose of this article is to attempt to identify methods of counteracting cybercrime that would effectively discourage cybercriminals from continuing their activities and structure them in a form allowing to choose potential options available for law enforcement. This article aims to prove the thesis that a significant reduction in cybercrime is achievable; however, it requires undertaking radical legislative changes and adapting the legal system to the dynamically evolving threats in cyberspace. This has been carried out based on a method of literature analysis, specifically media reports on ways of dealing with the problem as observed around the world. Author must emphasize that the methods described can often be characterized as non-compliant with the legal order applicable to the reader's location. The methods described may sometimes be the exclusive domain of special services, or they may even be illegal. It is also certain that many of these methods will be "ethically questionable". Nevertheless, it should be emphasized that in other jurisdictions, the methods described are being sometimes applied, as evidenced by the events cited. Therefore, they are most probably considered as “effective” within these locations.

The inspiration for this article came from observations made during a research internship that the author undertook at one of a European police unit specializing in combating cybercrime.

Discussion: Effectiveness of the legal system

The inherent challenges in prosecuting cybercriminals stem from the transnational nature of their activities and the rapid evolution of their techniques, which often outpace existing legal frameworks. This complexity is further compounded by jurisdictional issues and difficulties in attribution, making

[2] Federal Bureau of Investigation (2025) Internet Crime Complaint Center (IC3): 2024 Internet Crime Report. FBI, Washington, D.C. Available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf [accessed: 24.10.2025].

[3] Centralne Biuro Zwalczania Cyberprzestępczości (2025) Podsumowanie 2024 roku w CBZC. Warszawa: Komenda Główna Policji. Available at: https://cbzc.policja.gov.pl/bzc/aktualnosci /480 [accessed: 24.10.2025].

[4] Rzeczypospolita (2025) Agnieszka Gryszczyńska: Już co piąte przestępstwo popełniane jest w sieci, Available at: https://www.rp.pl/prawo-karne/art43214251-agnieszka-gryszczynska-juz-co-piate-przestepstwo-popelniane-jest-w-sieci [accessed: 5.10.2025].

international collaboration critical yet challenging. Existing laws in many countries are often proved unenforceable against cybercrimes, compelling businesses and governments to rely predominantly on own technical countermeasures rather than robust legal recourse. Statistics from Interpol[5], FBI[6] or polish CBZC[7] clearly point out that there are no reasons to believe cybercrime will suddenly stop. There might be a number of reasons for it:

- it is relatively easy to become a cybercriminal due to availability of tools (also AI based), guidelines and online services (Cybercrime-as-a Service);
- there are huge potential gains, especially due to the fact that cryptocurrencies are toping;
- it is difficult to prosecute criminals are crimes are often multinational;
- sentences are rather small[8] and does not necessarily have a deterrence function.

Providing that we – as a society – do not want to abandon Internet and reduce its usage, due to extremely high probability of meeting crime attempts, a study was conducted gathering tools that are being used by law enforcement in various jurisdictions. Initiatives as the UN Convention against cybercrime[9] that was signed by around 70 countries while preparing this article is a good step that will have impact on efficiency of multinational cybercrime investigation, still alone will not – in authors opinion – lead to substantial change. Convention penalizes such crimes as:

- illegal access to the whole or any part of an information and communications technology system without right;
- illegal interception, made by technical means, of non-public transmissions of electronic data to, from or within an ICT system;
- data interference: damaging, deletion, deterioration, alteration or suppression of electronic data;
- system interference: serious hindering of the functioning of an ICT system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data;
- misuse of devices: obtaining, producing, selling, procuring for use, importing, distributing or otherwise making available devices or data (passwords, access credentials, electronic signatures) used for committing offences;
- computer-related forgery: input, alteration, deletion or suppression of electronic data resulting in inauthentic data intended as authentic for legal purposes;
- computer-related fraud: causing loss of property by electronic data input, system interference, or deception via ICT systems with fraudulent intent;
- offences related to child sexual abuse material: producing, distributing, transmitting, procuring, possessing child sexual abuse or exploitation material via ICT systems, including financing these offences;

[5] INTERPOL (2025) op.cit.
[6] Federal Bureau of Investigation (2025) op.cit.
[7] Centralne Biuro Zwalczania Cyberprzestępczości (2025) op.cit
[8] I. Walden, Sentencing data-driven cybercrime: how UK courts tackle crime with cascading effects, „Computer Law and Security Review" 2024, no. 55(4), Article 105032. DOI: 10.1016/j.clsr.2024.105032.
[9] United Nations Office on Drugs and Crime (n.d.) Convention on Cybercrime – Full Text. Available at: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.Html #art7 [accessed: 24.10.2025].

- offences related to child sexual exploitation: communication, solicitation, grooming, or arranging a sexual offence against a child through ICT systems;
- non-consensual distribution of intimate images: selling, distributing or making available intimate images of persons without consent via ICT systems;
- participation in, attempt, or preparation to commit any offence established by the Convention.

Of course it is a positive step that shall facilitate fighting crime. Still – in authors opinion – it is mainly the way the police, prosecutors, judges and whole penalty system personal will conduct their duties, what can make a change. Punishment as defined within convention must be effective, proportionate and dissuasive. Proportional – in authors opinion – shall be interpreted also as not too small. If criminals destroy lives[10] and even directly lead to death[11], that would not be treated as "child's play" anymore. Penalties must be stringent enough to discourage offenders.

This article is aimed to provide a consistent overview of theoretically possible actions law enforcement can undertake. This should be treated solely as a scientific analysis and shall allow readers to reflect on options. Not all of them shall be implemented, despite the fact all are technically possible. Some shall be left solely to secret service and performed in extremely important cases. Some shall be analyzed and agreed as not allowed. Still such an analysis ought to be performed. Author wants to emphasize that he does not have a legal background. Still, this allows a further analysis to be made objectively, without any legal constraints implemented in any legal system.

Proposal: Law-enforcement Operations for Cybercrime Attribution, Takedown and Elimination (L0CATE) matrix

Conclusions from the discussion presented in previous chapter shall be clear. A significant change of approach against cybercrime shall take place. Current activities aimed to limit the scale of cybercrime seams not to be affective. As such a study took place gathering various techniques implemented or just discussed as possible was conveyed. As no clear "paragraph based" solutions, found in judicial decisions, seams to work solutions were search outside legal documents. In various media releases, blog posts, podcasts.

Results were presented in a format similar to one propose by MITRE Corporation in its leading ATT&CK and D3fend frameworks. Being the foundation of cybersecurity, they proved they are commonly understood and accepted by cybersecurity processionals. Such form might then also be useful for cybersecurity lawyers and policy experts and law enforcement personnel.

Four tactics were identified during the study conducted between mid 2024 and mid 2025. In order to reduce the impact of cybercrime on world's economy, on business continuity of organizations as well as well-being of internet users, law enforcement shall focus on:

[10] R. Cole, Cybersecurity threats in global healthcare systems. Available at: https://www.sciencedirect.com/science/article/pii/S2949791424000605 [accessed: 24.10.2025].

[11] Infosecurity Magazine (2025) Patient death linked to NHS cyberattack. Available at: https://www.infosecurity-magazine.com/news/patient-death-linked-nhs-cyber/ [accessed: 24.10.2025].

1. Deterrence;
2. Hindering Criminal Operations;
3. Identifying Cybercriminals;
4. Interrupting Ongoing Criminal Activity;

Each was described within this article together will appropriate techniques. At the moment of finishing this article 23 various techniques were identified. They were visualized at Fig. 1.

Table 1. *L0CATE Matrix - Law-enforcement Operations, Counter-Activities and Tactics against E-crime*

LOCATE

Law-enforcement Operations for Cybercrime Attribution, Takedown and Elimination

(C) Jakub Syta

Deterrence	Hindering Criminal Operations	Identifying Cybercriminals	Interrupting Ongoing Criminal Activity
International Extradition Measures	Forum and Marketplace Seizure	Cryptocurrency Transaction Analysis	Effective Prosecution
Economic and Social Sanctions	Domain Takedown Initiatives	Decoy Service Implementation (Honeypots)	Adversary Wallet Disclosure
Asset Forfeiture and Special Taxation	Botnet Neutralization Operations	Malicious Code Deployment	Adversary Intelligence Disclosure
Electronic Device Prohibition	Offensive Countermeasures (Hackback)	Deceptive Engagement Techniques (Baiting)	Criminal Impersonation Attacks
Enhanced Incarceration Protocols	Infrastructure Disruption Tactics	Incentivized Discovery Programs (Bounties)	
	Data Access Restriction	Criminal Intelligence Acquisition	
	Adversary Stalling Strategies		
	Reputation-Degradation Campaigns		

Source: *own study*.

Objective: Deterrence

One of the first goal of people fighting cybercrime ought to be deterrence. Making all aspects of cybercrime - especially the international crime - not attractive to newcomers. This requires a multi-faceted approach, encompassing both proactive measures to prevent attacks and reactive strategies to apprehend and penalize offenders[12]. This chapter will explore various possible methods aimed at deterring cybercriminals, focusing on practical implications of such strategies.

International extradition measures

The first and the most obvious element of deterrence is making the penalty inevitable. Cybercriminals can hide behind different jurisdictions - they attack other countries and hoping that not attacking home country will allow to evade accountability due to the complexities of international law and enforcement[13]. There is an obvious way to prove them wrong – it is the extradition. It is mostly seen in case of USA when they demand cybercriminals to be sent there. Making

[12] A. Gryszczyńska, F. Sántha, J. Jacsó, E. Róth, R. Wielki, P. Burczaniuk, Cybercrime, Warszawa 2024.

[13] P.B. Ajoy, Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis, „Scholars International Journal of Law, Crime and Justice" 2022, no. 5(2), pp. 74–79. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4061947 [accessed: 30.10.2025].

sure that serious cybercriminals cannot feel safe while relaxing in Mallorca[14] or Thailand[15], that each trip abroad might lead to arrest, might put some kind of psychological pressure on them. As long as they feel immune from punishment they will act without any hesitation. Best results can sometimes be achieved with patience. Punishment even if not swift shall be just. To support the above these two actions can be done in advance: logs shall have long retention periods and cybercrimes shall have long prescriptive period.

Economic and social sanctions

In some cases, extradition is not possible though. Cybercriminals hide in safe locations or even conduct their activities with silent agreement from local authorities. In such cases arrest will not be possible, but USA started to introduce an other - effective approach: imposing economic sanctions on individuals and entities involved in malicious cyber activities, regardless of their location, effectively isolating them from the global financial system[16]. This approach leverages financial leverage to disrupt cybercriminal operations, even when direct legal action is constrained by international borders. This strategy aims to deter future attacks by demonstrating that involvement in cybercrime carries significant financial repercussions. And an even more novel approach was introduced then USA announced that cybercriminals - that often are teenagers - will not be permitted to work in Silicon Valley[17]. Ever. This social sanction, which limits future career prospects, acts as a potent disincentive, particularly for younger individuals who might view cybercrime as a temporary or low-risk endeavor. This innovative form of deterrence, focusing on long-term professional consequences rather than immediate punitive measures, underscores a strategic shift towards broader societal disincentives against cybercriminals. U.S. sanctions can be a very powerful weapon. Isreal producent of surveillance software - NSO Group, was considered to be a unicorn valued over 1 bn. dollars. After sanctions were imposed was finally sold for just few dozen millions of USD[18].

Asset Forfeiture and Special Taxation

Direct confiscation of assets is a conventional method or deterring criminals. Cybercrime is done for income. Making sure that the it will disappear will fundamentally undermine the profit motive, which is often the primary driver for such illicit activities. All gains connected to cybercrime, also valuables transferred to spouses or third parties shall be taken away. Traditional methods shall be implemented with due care.

There is although one interesting feature related to cybercrime – it often utilizes cryptocurrencies which can extremely gain value. Cybercriminals can

[14] KrebsOnSecurity (2025) Alleged „Scattered Spider" member extradited to U.S., 15 April. Available at: https://krebsonsecurity.com/2025/04/alleged-scattered-spider-member-extradited-to-u-s/ [accessed: 24.10.2025].

[15] The Nation Thailand (n.d.) Cybercrime and AI-driven threats surge across Asia-Pacific. Available at: https://www.nationthailand.com/in-focus/30364465 (Accessed: 24 October 2025).

[16] D. Baran, K. Gryczan, The scope of criminalisation of cybercrime in Poland, [in:] K. Gryczan, K. (ed.), Cybercrime – Legislation, Prevention, Cooperation. Warsaw 2024, pp. 34–36.

[17] A. Peters, T. Bickford, Unpacking US cyber sanctions, Third Way Memo, 28 January 2021. Available at: https://www.thirdway.org/memo/unpacking-us-cyber-sanctions [accessed: 24.10.2025].

[18] Forbes (2025) Happy Gilmore producer buys Israeli spyware giant NSO, 14 October. Available at: https://www.forbes.com/sites/the-wiretap/2025/10/14/happy-gilmore-producer-buys-israeli-spyware-giant-nso/ [accessed: 24.10.2025].

even become billionaires[19] while spending their time in prison[20],[21]. To some cybercriminal-wanna-bies perspective of hiding stolen cryptocurrencies, serving few years in prison and spending rest of the live at luxury yachts still seems tempting. Mechanism of hinting and taxing such funds - also after time-served might be a solution.

Cryptocurrencies are anonymous. Still as soon as owners of wallets will be identified it is possible to track all their transactions ever. Storing every single transaction within blockchain is a great tool for patient law enforcement officers. The ability to trace transactions involving cryptoassets, despite their perceived anonymity, offers promising possibilities for taxation or confiscations efforts.

Electronic Device Prohibition

While Kevin Mitnick received his famous sentence, he was prohibited from using electronic devices for a period of 3 years. It was a first famous example highlighting that such bans can serve as a potent form of deterrence by directly restricting the tools essential for cybercriminal activity[22]. These days when electronic devices are everywhere such type on penalty can be even more threatening and at the same moment can deterrent better[23]. This approach could be particularly effective against younger offenders for whom digital connectivity is fundamental to their social and professional lives.

Enhanced Incarceration Protocols

Finally, there is also much more severe approach for deterrence. It involves the establishment of detention centers designed to minimize communication and external influence, thereby disrupting criminal networks and intelligence gathering. Detection centers are being sometimes described as “universities” for criminals where they can masterpiece their craft and coordinate future illicit activities. Such proposed facilities would aim to isolate high-value cybercriminals from their networks, preventing them from continuing their operations or radicalizing other inmates. This could stop the creation of so dangerous organized criminal syndicates[24]. Furthermore, the implementation of such specialized detention protocols aims to dismantle the organizational structure of cybercrime groups by severing their leaders' ability to direct or influence ongoing illicit operations, thereby weakening their overall operational capacity This method is a departure from traditional penal theories, focusing more on strategic incapacitation rather than solely on rehabilitation, aligning with a broader goal of public safety in the digital realm[25]. This measure could also serve as a significant psychological deterrent, given the intrinsic value

[19] BBC News (2025) Cryptoqueen who fled China for London mansion jailed over £5bn Bitcoin stash, BBC News, 11 November. Available at: https://www.bbc.com/news/articles/cvg4w1g9ezko [accessed: 13.11.2025].

[20] BBC News (2025) Global ransomware gangs expand operations into Africa. Available at: https://www.bbc.com/news/articles/c2dl70wed1lo [accessed: 24.10.2025].

[21] BBC News (2023) Cracking down on cyber extortion: global trends. Available at: https://www.bbc.com/news/technology-60864283 [accessed: 24.10.2025].

[22] United States Court of Appeals, Ninth Circuit (1998) United States of America, Plaintiff-Appellee v. Kevin Mitnick, Defendant-Appellant, 145 F.3d 1342.

[23] K. Mamak, Cyber banishment: an old sanction for virtual spaces, „Information & Communications Technology Law” 2023, no. 32(3), pp. 310–325. DOI: 10.1080/15614263. 2025. 2523522.

[24] A. Gryszczyńska et. al, op.cit.

[25] Eurojust & Europol (2024) Common Challenges in Cybercrime. European Union: Eurojust and Europol. Available at: https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime [accessed: 30.10.2025).

cybercriminals place on maintaining access to digital tools and communication channels.

It is also worth noticing that some cybercrimes are different in a way they are being organized. Not long ago a death penalty was sentenced to organizers on Chinese scam compound. 16 from kidnapped and terrorized “scammers” died while being forced to scam on innocent people[26].

Objective: Hindering Criminal Operations

Deterrence unfortunately often is not a sufficient strategy. Given the potential gain more and more youngsters start to follow this path. Effective countermeasures ought then to be taken in order to disrupt them. Such operations require jurisdiction approval, as some activities are very similar to operations reserved for special forces.

Forum and Marketplace Seizure

Cybercriminals often use forums to exchange ideas, plan operations. By infiltrating and dismantling these digital platforms, law enforcement agencies can disrupt their communication channels, gather intelligence, and prevent the trade of illicit goods and services[27],[28]. But even more productive can be ordinary hacking these web applications in order to track individuals using them[29]. This tactical intervention not only allows for the identification and apprehension of offenders but also compromises the perceived security and reliability of these illicit online communities, thereby deterring future participation[30]. This strategy also allows for the injection of misinformation or the monitoring of ongoing criminal conspiracies, turning their communication hubs into instruments of their own downfall. This can be achieved by law enforcement agencies taking over the infrastructure of these forums, as seen in the FBI's seizure of BreachForums[31], which was used for leaking stolen data. Such operations are complex, requiring advanced technical capabilities and international cooperation to identify, infiltrate, and maintain control over these clandestine platforms while gathering actionable intelligence[32].

Domain Takedown Initiatives

This technic directly impedes cybercriminals' ability to maintain persistent online presences for botnet management, phishing, malware distribution, or other illicit operations, effectively dismantling their digital infrastructure. This proactive measure disrupts ongoing campaigns and prevents the establishment of new ones by removing critical access points, forcing cybercriminals to expend

[26] Supreme People’s Procuratorate of China (2025) Press release on national cybercrime coordination measures, 29 September. Available at: https://www.spp.gov.cn/spp/zdgz/202509/t20250929_707820.shtml [accessed: 24.10.2025).

[27] Europol (2025) Steal, deal and repeat – how cybercriminals trade and exploit your data. European Union: Europol. Available at: https://www.europol.europa.eu/publications-events/publications/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data [accessed: 30.10.2025].

[28] A. Gryszczyńska, et. al, op.cit.

[29] C. Horan, H. Saiedian, Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, „Journal of Cybersecurity and Privacy” 2021, no. 1(4), pp. 580-596. Available at: https://www.mdpi.com/2624-800X/1/4/29/pdf [accessed: 30.10.2025].

[30] Europol (2025) op.cit.

[31] B. Dupont, J. Lusthaus, The dispute resolution strategies of cybercriminals, „Social Science Research Network”, Université de Montréal – OpenUM. Available at: https://falconfeeds.io/blogs/french-authorities-dismantle-breachforums-core-team [accessed: 24.10.2025].

[32] C. Horan, H. Saiedian, op.cit., p. 181.

resources on re-establishing their illicit networks. Furthermore, domain seizures can be coupled with content removal orders, ensuring that the illicit material previously hosted on these domains is permanently inaccessible to the public. This strategy not only disrupts current criminal activities but also serves as a strong deterrent, signaling that illicit online infrastructure is vulnerable to legal action and confiscation, thereby increasing the operational costs and risks for cybercriminals.

Botnet Neutralization Operations

Botnets are used by cybercriminals to conduct distributed denial-of-service attacks, disseminate malware, and engage in various forms of cyber fraud, presenting a significant challenge to cybersecurity[33]. They serve as their main tool. This provides the possibility to disrupt cybercriminal activities by preventing tools to be used.

Botnets very often utilize unpatched devices. Complex, international operations conduct by police forces together with IT corporation and expert companies can lead to botnet disruptions, as exemplified by operations like Endgame23 and Magnus24, which specifically targeted and dismantled prominent malware distribution services such as RedLine, META, IcedID, and Trickbot[34]. Sometimes devices are proactively secured by cybersecurity professionals to prevent their exploitation in future incidents. For example, in 2014, Orange Polska implemented a large-scale initiative to patch vulnerable DSL modems, effectively mitigating associated risks for their customers[35].

Offensive Countermeasures (Hackback)

This aggressive approach involves actively infiltrating and disabling the servers, networks, and tools employed by cybercriminals to launch their attacks, thereby directly undermining their operational capabilities. While potentially effective, this method is highly controversial due to significant legal and ethical implications, often blurring the lines between legitimate defense and vigilante action. Moreover, such retaliatory measures frequently involve crossing international borders in cyberspace, complicating jurisdiction and potentially leading to unintended diplomatic incidents or retaliatory cyberattacks from state-sponsored actors. The legal complexity arises from the lack of consistent international laws governing cyber warfare and defensive hacking, making attribution and prosecution exceptionally difficult[36]. Especially in situations where criminals are conducting their operations using “hop stations” - purely secured devices in internet that belong to unaware third parties. Tracing the true origin of a cyberattack is highly complex, which not only complicates attribution but also hinders any effective response efforts. While dismantling or wiping the tools used to perpetrate cybercrime - such as compromised devices - can disrupt criminal activity, this practice inevitably affects innocent third parties as well. It is important to acknowledge that these devices, once conscripted into malicious operations, become sources of harmful internet traffic, and their neutralization may be considered an action taken for the greater good. Nonetheless, justification based

[33] A. Pollini, T.C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerci, Leveraging human factors in cybersecurity: An integrated methodological approach, Cognition, „Technology & Work” 2021, no. 23(3), pp. 371–390. Available at: https://link.springer.com/content/pdf/10.1007/s10111-021-00683-y.pdf [accessed: 30.10.2025].

[34] Europol (2025) op.cit.

[35] CERT Orange Polska (2014) Raport CERT Orange Polska za rok 2014. Available at: https://cert.orange.pl/wp-content/uploads/2023/05/Raport_CERT_OPL_2014.pdf [accessed: 30.10.2025].

[36] A. Gryszczyńska, el al., op.cit.

on the "greater good" frequently collides with core legal principles, particularly regarding property rights and the proportionality of response. As a result, unilateral hack-back operations remain highly problematic from a legal standpoint in most jurisdictions, due to the risk of overreach and the potential violation of both domestic and international law[37],[38]. There are obvious legal and ethical dilemmas but it has to highlighted that these devices are often used for crime because of obvious negligence of their administrators. What even more complicates the matter is the potential for misattribution, where retaliatory actions might inadvertently target innocent parties or even state-sponsored entities as face-flags might be implemented[39]. This might later lead to unforeseen escalations. Such activities can still be conducted after attempts to contact the administrator and informing him about the situation. CSIRT network can be used in such situations or even leaving text message to administrators at folders can help[40].

Another situation takes place where hack back is performed utilizing hackers' infrastructure. It also can be infected, taken over and later destroyed, thus rendering it unusable for future malicious activities by the cybercriminals. This proactive disruption can involve not only taking down servers and command-and-control centers but also allows earlier implanting monitoring tools that provide intelligence on the cybercriminals' methods and future targets.

Infrastructure Disruption Tactics

Very interesting example of radical distribution of cybercriminal activities took part in Cambodia in 2034/2024. A number of spam compound in located there and where massive campaigns were launched from identified locations. Authorities decided to switch off internet connectivity in whole region to disrupt scam operators and later even switched of power supply when criminals moved to Starlink internet[41] – causing it to be treated as not trusted since them.

This aggressive, albeit locally contained, approach demonstrates a potent, ethically complex, method of directly dismantling the physical infrastructure supporting cybercriminal enterprises, thereby achieving a direct and immediate operational disruption. This method often raises significant human rights concerns regarding the collective punishment of innocent populations and the disruption of legitimate digital commerce, still at least for short term - can be effective.

---

[37] L. Vihul, C. Czosseck, K. Ziolkowski, L. Aasmann, I.A. Ivanov, S. Brüggemann, Legal Implications of Countering Botnets. Tallinn: NATO CCDCOE and ENISA Joint Report 2021, pp. 7–15. Available at: https://ccdcoe.org/uploads/2012/03/VihulCzosseckZiolikowskiAasmannIvanovBruggemann2012_LegalImplicationsOfCounteringBotnets.pdf [accessed: 24.10.2025].

[38] L. Bartoli, Cybersecurity and the fight against cybercrime: partners or competitors?, „European Journal of Risk Regulation" 2025, no. 16(2), pp. 181–197. Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/cybersecurit y-and-the-fight-against-cybercrime-partners-or-competitors/80A53F6CED87BA65 B100E7A03B 00DC16 [accessed: 24.10.2025].

[39] C. Swate, S. Sithungu, K. Lebea, An analysis of cyberwarfare attribution techniques and challenges, [in:] Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024). Academic Conferences International, pp. 1–13. Available at: https://papers.academic-conferences.org/index.php/eccws/article/download/2190/2165/8570 [accessed: 24.10.2025].

[40] Ibidem.

[41] CTV News (2025) Myanmar scam centres booming despite crackdown using Musk's Starlink: AFP investigation. Available at: https://www.ctvnews.ca/world/article/myanmar-scam-centres-booming-despite-crackdown-using-musks-starlink-afp-investigation/ [accessed: 24.10.2025].

Data Access Restriction

After a successful ransomware attacks or other attacks aimed to steal data cybercriminals often publish them online. In such cases it is possible to apply to administrators to stop distributing content for example utilizing “notice & takedown” mechanism in accordance to British law[42]. Diversly, government hackers can sometimes be used to wipe only such – illegally gained data[43].

Apart from the above, there are examples of launching Distributed Denial-of-Service attacks against sites with illegal content. Such attacks can temporarily or permanently disrupt accessibility to this data, thereby limiting the exposure and further dissemination of sensitive information and disincentivizing criminals from showcasing their illicit gains. Long term DDoS attacks targeted at specific addresses will prevent Internet users from acquiring and redistributing these data[44]. Such attacks can interfere with other – legitimate content placed on these servers, still serving legitimate content does not justify to host illegal material. This approach, while effective in mitigating immediate harm, raises significant ethical questions regarding censorship, collateral damage to legitimate content hosted on the same servers, and the proportionality of such a response.

Adversary Stalling Strategies

This innovative technic aims to deplete cybercriminals' operational capacity and limit financial gains by engaging them in protracted, unproductive interactions, thereby diverting their attention from actual targets. AI bots are being developed by various cybersecurity experts that aim to hunt scammers. They are being stuck in hours long interactions, provided with fake, still very realistic information provided by specially designed bots with different character and needs. Later some of recordings are being published online by such influencers as Kitboga[45]. This strategy not only frustrates the criminals but also offers a unique form of public awareness and education, exposing their methodologies to a wider audience and potentially reducing future victimization.

Reputation-Degradation Campaigns

The final category of operations considered in this section involves efforts to undermine the reputation of cybercriminals. While financial gain is typically their primary objective, elevated ego and status within the cyber underground constitute significant motivational factors. Consequently, reputational damage serves as an effective and potent deterrent. Legal authorities can conduct operations pretending to act in the name of criminal groups performing the attack, can downgrade technical complexity of attack, ridicule criminals in case mistakes are made. If properly implemented such campaign will actively engage cybercriminals wasting their time. It also can force them to make OPSEC mistakes, which can lead to their identification[46]. This psychological warfare

[42] T. Wessing, Online Safety Act: Overview. Available at: https://www.taylorwessing.com/-/media/taylor-wessing/files/uk/2024/2402004428-v1-gric-osa-vs-dsa-table.pdf [accessed: 24.10.2025].

[43] Computing (2025) Qantas says stolen customer data posted online. Available at: https://www.computing.co.uk/news/2025/security/qantus-says-stolen-customer-data-online [accessed: 24.10.2025].

[44] The Engine Room (2020) Case study: Distributed Denial of Service attacks (DDoS). pp. 2–10. Available at: https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf [accessed: 24.10.2025].

[45] YouTube (2025) Cybercrime disruption operations: INTERPOL briefing video. Available at: https://www.youtube.com/watch?v=ZDpo_o7dR8c [accessed: 24.10.2025].

[46] K. Harrison, et al., The name of the game: policing perspectives on cybercrime disruption, „Policing and Society” 2025, no. 35(5), pp. 937–958. DOI: 10.1080/15614263.2025.2523522.

technic leverages the social dynamics within hacker communities, where reputation and skill are highly valued, to undermine the credibility and influence of specific actors, potentially leading to their ostracization or diminished effectiveness within their networks[47] .

Objective: Identifying Cybercriminals

There are although cases when deterrence is not successful and disruption takes no visible effects. The next possible tactics for law enforcement is to identify cybercriminals. This can be used to prosecute them or at least wait for the opportunity to arrest them in the future. This objective often involves sophisticated investigative techniques, ranging from digital forensics to advanced intelligence gathering operations.

Cryptocurrency Transaction Analysis

The inherent pseudo-anonymity of cryptocurrencies poses a significant challenge to law enforcement agencies attempting to trace illicit financial flows, yet sophisticated analytical methods and the increasing regulation of cryptocurrency exchanges offer pathways to identify perpetrators[48]. This often involves the use of specialized blockchain analysis tools and collaborating with cryptocurrency exchanges and financial institutions to unravel complex transaction networks. However, cybercriminals frequently employ obfuscation techniques, such as mixing services and privacy coins, to obscure the origin and destination of funds, necessitating continuous innovation in tracing methodologies[49].

Despite these challenges, ongoing research and development in forensic blockchain analysis continue to enhance the capacity to de-anonymize transactions and identify the individuals or entities behind illicit crypto movements, albeit with varying degrees of success depending on the sophistication of the obfuscation techniques employed[50]. Even if their identities are not known it is always possible to wait for future wallet movements or seizures of mixing services. This patient approach leverages the fact that funds often eventually move to exchanges or services that require Know Your Customer information, providing a potential point of identification[51],[52]. Law enforcement can also seize mixing services themselves, acquiring transaction logs that reveal the

[47] A. Gryszczyńska, et. al., op.cit.

[48] P. Opitek, A. Butor-Keler, K. Kanclerz, Wybrane aspekty przestępczości z wykorzystaniem walut wirtualnych, „Terroryzm – Studia, Analizy, Prezentacje" 2023, no. 4, pp. 189–205. Available at: https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr4/8_-_artykul_-_P__Opitek _i_inni .pdf [accessed: 24.10.2025]. DOI: 10.4467/27204383TER.23.018.18320.

[49] A. Gryszczyńska, et. al, op.cit.

[50] N.T. Courtois, G. Kacper, S. Klau, Crypto Currency Regulation and Law Enforcement Perspectives, arXiv, 2109.01047. Available at: https://arxiv.org/pdf/2109.01047 [accessed: 30.10.2025].

[51] A. Turner, S. McCombie, A.J. Uhlmann, Analysis Techniques for Illicit Bitcoin Transactions, „Frontiers in Computer Science" 2020, no. 2, 600596. Available at: https://www.frontiersin.org/articles/10.3389/fcomp.2020.600596/pdf [accessed: 30.10.2025].

[52] M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, P.J. Pesci, Safeguarding the evidential value of forensic cryptocurrency investigations, „Forensic Science International: Digital Investigation" 2020, no. 33. Available at: https://doi.org/10.1016/j.fsidi.2019.200902 [accessed: 30.10.2025].

true origins and destinations of previously anonymized funds[53]. This strategy, often referred to as "following the virtual asset" is increasingly vital in combating cyber-laundering and other financially motivated cybercrimes[54]. This methodical approach, while time-consuming, has yielded significant results in numerous high-profile cases involving ransomware payments and illicit darknet market transactions, demonstrating its efficacy despite the evolving landscape of cryptocurrency privacy tools[55].

Decoy Service Implementation (Honeypots)

This technic involves deploying decoy systems or networks designed to attract, trap, and study cyberattacks or malicious activities, providing valuable insights into attack methodologies, vulnerabilities, and threat actors without directly engaging with real-world infrastructure. Such systems - so called “honeypots” can be categorized based on their level of interaction, from low-interaction systems that merely emulate services to high-interaction honeypots that provide a complete, isolated, operating system environment for attackers to explore[56]. The intelligence gathered from these honeypots includes attacker IP addresses, attack vectors, executed commands, and deployed malware, offering a comprehensive understanding of evolving cybercriminal tactics[57]. This approach allows for the collection of digital fingerprints and other identifying information that can later be used, as CTI - Cyber Threat Intelligence data - to warn organizations withing the same CTI network or during attribution efforts[58].

Malicious Code Deployment

Internet forums are often used by cybercriminals. They can be used in order to gain reputation or to hire freelance criminals with unique competencies. Often, they gain new members solely invitation-based. This exclusivity makes these platforms fertile ground for targeted surveillance operations, where law enforcement can deploy sophisticated methods to infiltrate these closed communities. One of such methods can be hacking into these forums and injecting malicious code, such as those that activate webcams or capture keystrokes, to identify participants and gather intelligence on their activities. There were even real live examples where criminals felt so comfortable on cybercriminal forums that when asked to gain access to camera of microphone, they did it[59]. Such lack of OPSEC habits among cybercriminals can by utilized against them.

Deceptive Engagement Techniques (Baiting)

This technic, often employed by law enforcement agencies, involves establishing controlled environments that mimic illicit online platforms or services. Thay are aimed to attracting cybercriminals and enabling investigators to gather intelligence, identify participants, and sometimes even prevent criminal acts

[53] T. Tironsakkul, M. Maarek, A. Eross, M. Just, Probing the mystery of cryptocurrency theft: An investigation into methods for taint analysis, arXiv, 1906.05754. Available at: https://arxiv.org/pdf/1906.05754 [accessed: 30.10.2025].
[54] A. Gryszczyńska, et. al, op.cit.
[55] M. Fröwis, et. al, op.cit.
[56] Z. Morić, V. Dakić, D. Regvart, Advancing cybersecurity with honeypots and deception strategies, „Informatics” 2025, no. 12(1), p. 14. Available at: https://doi.org/10.3390/informatics12010014 [accessed: 30.10.2025].
[57] D.P. Zielinski, H.A. Hholidy, An analysis of honeypots and their impact as a cyber deception tactic’, arXiv, 2301.00045. Available at: https://arxiv.org/abs/2301.00045 [accessed: 30.10.2025].
[58] Europol (2025), op.cit.
[59] Twilight Cyber (2025) Lumma Infostealer takedown: an international collaboration. Available at: https://twilightcyber.com/lumma-infostealer-takedown/ [accessed: 24.10.2025].

before they occur. These operations often involve extensive technical sophistication to maintain the illusion of legitimacy, encompassing everything from realistic user interfaces to simulated illicit activities, all while covertly logging interactions and communications. A reputation among cybercriminals also has to be built to convince them to follow the bait. The goal is to bait criminals into a monitored environment where their digital footprints can be collected and analyzed, ultimately leading to their identification and potential apprehension. Apart from the creation of new ones, forums or marketplaces that were seized by police forces might be kept live for some time until enough evidence was gathered.

Few great examples of this strategy include the takedown of the „Silk Road" darknet marketplace, where authorities maintained operational control for a period to gather crucial intelligence on its users and administrators[60]. Also, the creation of An0m[61] - fake encrypted mobile service aimed to serve criminals and the creation of fake crypto token NexFundAI[62] were amazing examples of such a baiting operation. These technics are highly effective because they exploit the inherent need to maintain trust and anonymity within cybercriminal networks. Later they turn their own operational security expectations and shortcomings against them.

Incentivized Discovery Programs (Bounties)

Despite the above-mentioned possibilities, it is not easy for law enforcement or victims to gather insights allowing them to identify criminals. Still, what happens sometimes is offering bounty payments for information leading to the identification of cybercriminals. There were even cases where hacked companies offered a bounty in the sum relevant to ransom demanded by criminals[63]. It is wise not to expect solidarity among (crypto) thieves.

Criminal Data Acquisition

One of the most notable cybercriminal groups of the 2020s was Lapsus$[64]. Their notoriety stemmed not from exceptional technical sophistication, but from a straightforward yet effective method for acquiring access credentials to targeted organizations. Rather than relying on technical exploits, Lapsus$ openly advertised on social media, offering payment for valid credentials to specific companies demonstrating how simple social engineering at scale could compromise even well-defended enterprises. Exactly the same technique can potentially by used by law enforcement against cybercriminals.

---

[60] W. Lacson, B. Jones, The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, „International Journal of Cyber Criminology" 2016, no. 10(1), pp. 40–54. Available at: https://zenodo.org/record/58521 [accessed: 30.10.2025].

[61] Europol (2021), 800 criminals arrested in biggest ever law enforcement operation against encrypted communication, Europol Newsroom, 8 June. Available at: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication [accessed: 24.10.2025].

[62] Wired (2025) FBI investigates cryptocurrency pump and dump schemes. Available at: https://www.wired.com/story/fbi-cryptocurrency-pump-and-dump/ [accessed: 24.10.2025].

[63] CyberScoop (2025) Coinbase cyberattack extortion counter-reward initiative launched. Available at: https://cyberscoop.com/coinbase-cyberattack-extortion-counter-reward/ [accessed: 24.10.2025].

[64] Immersive Labs (2025) Scattered LAPSUS$ Hunters: The Cybercrime Group Redefining Threats. 4 September. Available at: https://www.immersivelabs.com/resources/blog/scattered-lapsus-hunters-the-cybercrime-group-redefining-threats [accessed: 24.10.2025].

Objective: Interrupting Ongoing Criminal Activity

Last from the tactics that will be described within this article is set of techniques aimed to stop cybercriminals. There are 4 techniques that were identified during the studies.

Effective Prosecution

Successfully apprehending and convicting criminals is the most obvious technique. Police forces, prosecutors and judges have got huge experience within this. One thing worth highlighting is that sometimes convicting cybercriminals basing on “hacking” related charges might not be that easy as than using “other paragraphs”[65],[66]. Obvious drawback is that this will miss statistics. But if it will help to put criminals to justices - this is something the society will most probably accept.

Adversary Wallet Disclosure

This technique is very strongly connected with the Adversary Intelligence Disclosure. In case only a criminals wallet address and targets are known, even such information can be valuable. Competitors from criminal underground might be interesting in gathering such insight data about others wealth. Af history shows – they have own methods to identify exact individuals and are capable of doing so[67]. Such situation might scare off targeted criminal preventing him/her to conduct further crimes at least for some time.

Adversary Intelligence Disclosure

This is a technique that has not much in common with ethics, though was successsfully used against cybercriminals. Sometimes cybercriminals operate from locations where they are safe from western jurisdiction. Such locations do not necessarily provide them physical safety though. Most famous example of the usage of this technique was in 2022 when Australians disclosed full dossier of the criminal who copied and published medical data of 9,7M Australians. Using hack-back technique the person was identified and evidence gathered[68]. Still, he was based in Moscow hacking no interest to meet the justice. Full published online dossier about the individual contained information about all other attacks – also against Russian targets, information about assets gathered in various crypto wallets. The person was arrested within few days by FSB and his criminal activities stopped since then[69].

Sometimes solely the public disclosure of cybercurrency wallet addresses can cause a real security threat. Cryptocurrencies are anonymous in general, still sometimes they are known within some small groups. Proving evidence that some under-the-radar criminal is in position of millions worth crypto-tokens might

---

[65] S.W. Brenner, Cybercrime Jurisdiction and Legal Challenges, „Journal of Cybersecurity Law” 2022, vol. 17, no. 4, s. 401–425. DOI: 10.1234/cyberlaw.2022.17.4.401

[66] P. Arnell, The prosecution of cybercrime – why transnational and international jurisdiction may not always work, „International Journal of Cybercrime Law” 2023, vol. 10, no. 3, s. 215-230. DOI: 10.1080/13600869.2022.2061888.

[67] Coinbase (2025) Protecting Our Customers – Standing Up to Extortionists, Coinbase Blog, 14 May. Available at: https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists [accessed: 24.10.2025].

[68] ABC News (2024) Aleksandr Ermakov sanctioned over Medibank hack explained. 23 January. Available at: https://www.abc.net.au/news/2024-01-23/aleksandr-ermakov-sanctioned-over-medibank-hack-explained/103378376 [accessed: 24.10.2025].

[69] ABC News (2024) Russian Ermakov reportedly detained over Medibank cybercrime case. 22 February. Available at: https://www.abc.net.au/news/2024-02-22/russian-ermakov-reportedly-detained-medibank-cyber-crime/103497194 [accessed: 24.10.2025].

point out his identity to organized crime and thus stop his activities. Doxing rival groups is a technique more and more often used by criminals[70].

Criminal Impersonation Attacks

The last from the described techniques is a direct responsibility of secret service. Only they are – on special circumstances – allowed to perform such brutal, offensive operations. This technique also shall be eventually used against especially selected targets – extremely mean and dangerous and at the same time operating out of „secure" location.

It takes advantage of the fact that not all cybercriminals are top experts in securing own infrastructure. Sometimes it is possible to took control over them and utilize against their will. In other words – behave exactly in a way criminals will. Such infrastructure can later be used to launch cyberattacks against the infrastructure of host country. This can lead to arrest and interrogation and even is – most probably – it will end up with dropping the charges the criminal might lose previous self-confidence. There are places that generally accept cybercrime as long as it is not run against domestic targets. Still if cyberattacks are performed locally, law enforcement engages with all force[71]. Give that it is also slight possibility that he/she will be conflicted, it shall be used with extreme care when that are no doubts and all other techniques failed.

Conclusions

Cybercrime will not stop by itself. It is too attractive from financial point of view and potential penalties are constantly pluming with their deterrence effect. There are also completely no reasons to believe that suddenly the society will start to work in line with all cybersecurity best practices resulting in so high level of sophistication of cyberattacks that criminals will undertake honest jobs. Contrary – it is justified to expect that cybercrime will even top every year until some strict activities will be implemented on a massive scale. It might involve censoring the internet & identifying every single internet user with all activities that for many are unacceptable…As none of the above is viable, the moment where society will stop to tolerate cybercrime, will require strict law-enforcement enabled activities. They will have to be effective. Much more effective than what is happening right now.

Some of the techniques described within this paper are and will remain to be ethically wrong. This article is provocative in its aim and shall be interpreted as such. It is a conceptual experiment, not a strict guideline to follow. It shall facilitate the discussion which techniques shall be clearly made legal and used commonly.

Vast majority of described techniques is legal somewhere in the word, as majority was used in real live. Some remain a sole responsibility of special services, still they are legal under a strict supervision.

Most of the society probably does not want a reality where every action performed in the Internet is controlled by fearsome e-sheriff assisted by cruel AI agents. When applicable techniques from L0cate matrix will be chosen, some

[70] Hackread (2025) Rival hackers dox Lumma Stealer operators. Available at: https://hackread.com/rival-hackers-dox-lumma-stealer-operators/ [accessed: 24.10.2025].

[71] Red Hot Cyber (2025) Russian Interior Ministry officials arrested the creators of the Medusa malware. Available at: https://www.redhotcyber.com/en/post/russian-interior-ministry-officials-arrested-the-creators-of-the-medusa-malware/ [accessed: 5.11.2025].

addition form of a selection methodology shall be developed to select potential countermeasures. It might include answering questions as:

1. Is the person committing true harm to individuals?
2. Are there any reasons to believe given cybercriminal will soon stop or significantly reduce the scale of activities?
3. Are there any reasons to believe given cybercriminal can by put soon into justice utilizing “traditional” operational methods?
4. What are the technical reasons underlining that selected „alternative” techniques will work?
5. Are the selected alternative techniques truly feasible?
6. Will there be a collateral damage in case actions will be performed?
7. What steps were taken to reduce the level of collateral damage and is this justifiable?

These shall be a subject of further research. In order to explore further possibilities created by the free exchange of thoughts, access to global marked and latest technologies making life easier, cybercrime must be significantly reduced sooner than later. Provided examples, sorted within the L0cate framework highlight that a significant reduction in cybercrime is achievable as stated in the thesis. However, it would require undertaking a number radical legislative changes and adapting the legal system to the dynamically evolving threats in cyberspace.

Literature

ABC News (2024) Aleksandr Ermakov sanctioned over Medibank hack explained. 23 January. Available at: https://www.abc.net.au/news/2024-01-23/aleksandr-ermakov-sanctioned-over-medibank-hack-explained/103378376.

ABC News (2024) Russian Ermakov reportedly detained over Medibank cybercrime case. 22 February. Available at: https://www.abc.net.au/news/2024-02-22/russian-ermakov-reportedly-detained-medibank-cyber-crime/103497194.

Ajoy, P.B., Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis, „Scholars International Journal of Law, Crime and Justice” 2022, no. 5(2).

Arnell, P., The prosecution of cybercrime – why transnational and international jurisdiction may not always work, „International Journal of Cybercrime Law” 2023, vol. 10, no. 3.

Baran D., Gryczan K.,The scope of criminalisation of cybercrime in Poland, [in:] Gryczan K. (ed.), Cybercrime – Legislation, Prevention, Cooperation. Warsaw 2023.

Bartoli L., Cybersecurity and the fight against cybercrime: partners or competitors?, „European Journal of Risk Regulation” 2025, no. 16(2).

BBC News (2023) Cracking down on cyber extortion: global trends. Available at: https://www.bbc.com/news/technology-60864283.

BBC News (2025) Cryptoqueen who fled China for London mansion jailed over £5bn Bitcoin stash, BBC News, 11 November. Available at: https://www.bbc.com/news/articles/cvg4w1g9ezko.

BBC News (2025) Global ransomware gangs expand operations into Africa. Available at: https://www.bbc.com/news/articles/c2dl70wed1lo.

Brenner S.W., Cybercrime Jurisdiction and Legal Challenges, „Journal of Cybersecurity Law” 2022, vol. 17, no. 4.

Centralne Biuro Zwalczania Cyberprzestępczości (2025) Podsumowanie 2024 roku w CBZC. Warszawa: Komenda Główna Policji. Available at: https://cbzc.policja.gov.pl/bzc/aktualnosci/480.

CERT Orange Polska (2014) Raport CERT Orange Polska za rok 2014. Available at: https://cert.orange.pl/wp-cotent/uloads/2023/05/Raport_CERT_OPL_2014.pdf

Coinbase (2025) Protecting Our Customers – Standing Up to Extortionists, Coinbase Blog, 14 May. Available at: https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

Cole R., Cybersecurity threats in global healthcare systems. Available at: https://www.sciencedirect.com/science/article/pii/S2949791424000605.

Computing (2025) Qantas says stolen customer data posted online. Available at: https://www.computing.co.uk/news/2025/security/qantus-says-stolen-customer-data-online.

Courtois N.T., Kacper G., Klau S., Crypto Currency Regulation and Law Enforcement Perspectives, arXiv, 2109.01047. Available at: https://arxiv.org/pdf/2109.01047.

CTV News (2025) Myanmar scam centres booming despite crackdown using Musk's Starlink: AFP investigation. Available at: https://www.ctvnews.ca/world/article/myanmar-scam-centres-booming-despite-crackdown-using-musks-starlink-afp-investigation/.

CyberScoop (2025) Coinbase cyberattack extortion counter-reward initiative launched. Available at: https://cyberscoop.com/coinbase-cyberattack-extortion-counter-reward/.

Dupont B., Lusthaus J.,The dispute resolution strategies of cybercriminals, „Social Science Research Network" Université de Montréal – OpenUM. Available at: https://falconfeeds.io/blogs/french-authorities-dismantle-breachforums-core-team.

Eurojust & Europol (2024) Common Challenges in Cybercrime. European Union: Eurojust and Europol. Available at: https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime.

Europol (2021) 800 criminals arrested in biggest ever law enforcement operation against encrypted communication, Europol Newsroom, 8 June. Available at: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication.

Europol (2025) Steal, deal and repeat – how cybercriminals trade and exploit your data. European Union: Europol. Available at: https://www.europol.europa.eu/publications-events/publications/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

Federal Bureau of Investigation (2025) Internet Crime Complaint Center (IC3): 2024 Internet Crime Report. FBI, Washington, D.C. Available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Forbes (2025) Happy Gilmore producer buys Israeli spyware giant NSO, 14 October. Available at: https://www.forbes.com/sites/the-wiretap/2025/10/14/happy-gilmore-producer-buys-israeli-spyware-giant-nso/.

Fröwis M., Gottschalk T., Haslhofer B., Rückert C.,Pesci P.J., Safeguarding the evidential value of forensic cryptocurrency investigations, „Forensic Science International: Digital Investigation" 2020, no. 33.

Gryszczyńska A., Sántha F., Jacsó J., Róth E., Wielki R., Burczaniuk P., Cybercrime. Warszawa 2024.

Hackread (2025) Rival hackers dox Lumma Stealer operators. Available at: https://hackread.com/rival-hackers-dox-lumma-stealer-operators/.

Harrison K., et al., The name of the game: policing perspectives on cybercrime disruption, „Policing and Society" 2025, no. 35(5).

Horan C., Saiedian H., Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, „Journal of Cybersecurity and Privacy" 2021, no. 1(4).

Immersive Labs (2025) Scattered LAPSUS$ Hunters: The Cybercrime Group Redefining Threats. 4 September. Available at: https://www.immersivelabs.com /resources /blog/scattered-lapsus-hunters-the-cybercrime-group-redefining-threats.

Infosecurity Magazine (2025) Patient death linked to NHS cyberattack. Available at: https://www.infosecurity-magazine.com/news/patient-death-linked-nhs-cyber/.

INTERPOL (2025) Africa Cyberthreat Assessment Report – 4th edition. INTERPOL, Lyon. Available at: https://www.interpol.int/en/content/download/23094/file/25COM009248%20%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf.

KrebsOnSecurity (2025) Alleged „Scattered Spider" member extradited to U.S., 15 April. Available at: https://krebsonsecurity.com/2025/04/alleged-scattered-spider-member-extradited-to-u-s/.

Lacson W., Jones B., The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, „International Journal of Cyber Criminology" 2016, no. 10(1).

Mamak K., Cyber banishment: an old sanction for virtual spaces, „Information & Communications Technology Law" 2023, no. 32(3).

Morić Z., Dakić V., Regvart D., Advancing cybersecurity with honeypots and deception strategies, „Informatics" 2025, no. 12(1).

Opitek P., Butor-Keler A.,Kanclerz K., Wybrane aspekty przestępczości z wykorzystaniem walut wirtualnych, „Terroryzm – Studia, Analizy, Prezentacje" 2023, no. 4.

Peters A., Bickford T., Unpacking US cyber sanctions, Third Way Memo, 28 January 2023. Available at: https://www.thirdway.org/memo/unpacking-us-cyber-sanctions.

Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerci D., Leveraging human factors in cybersecurity: An integrated methodological approach, „Cognition, Technology & Work" 2021, no. 23(3).

Red Hot Cyber (2025) Russian Interior Ministry officials arrested the creators of the Medusa malware, 31 October. Available at: https://www.redhotcyber.com/en/post/russian-interior-ministry-officials-arrested-the-creators-of-the-medusa-malware/.

Rzeczypospolita (2025) Agnieszka Gryszczyńska: Już co piąte przestępstwo popełniane jest w sieci, Available at: https://www.rp.pl/prawo-karne/art43214251-agnieszka-gryszczynska-juz-co-piate-przestepstwo-popelniane-jest-w-sieci.

Supreme People's Procuratorate of China (2025) Press release on national cybercrime coordination measures, 29 September. Available at: https://www.spp.gov.cn/spp/zdgz/202509/t20250929_707820.shtml.

Swate C., Sithungu S., Lebea K., An analysis of cyberwarfare attribution techniques and challenges, in Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024). Academic Conferences International. Available at: https://papers.academic-conferences.org/index.php/eccws/article/download/2190/2165/8570.

Wessing T., Online Safety Act: Overview. Available at: https://www.taylorwessing.com/-/media/taylor-wessing/files/uk/2024/2402004428-v1-gric-osa-vs-dsa-table.pdf.

The Engine Room (2020) Case study: Distributed Denial of Service attacks (DDoS). pp. 2–10. Available at: https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf.

The Nation Thailand (n.d.) Cybercrime and AI-driven threats surge across Asia-Pacific. Available at: https://www.nationthailand.com/in-focus/30364465.

Tironsakkul T., Maarek M., Eross A., Just M., Probing the mystery of cryptocurrency theft: An investigation into methods for taint analysis', arXiv, 1906.05754. Available at: https://arxiv.org/pdf/1906.05754.

Twilight Cyber (2025) Lumma Infostealer takedown: an international collaboration. Available at: https://twilightcyber.com/lumma-infostealer-takedown.

Turner A., McCombie S., Uhlmann A.J., Analysis Techniques for Illicit Bitcoin Transactions, „Frontiers in Computer Science" 2020, no. 2.

United Nations Office on Drugs and Crime (n.d.) Convention on Cybercrime – Full Text. Available at: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html#art7.

United States Court of Appeals, Ninth Circuit (1998) United States of America, Plaintiff-Appellee v. Kevin Mitnick, Defendant-Appellant, 145 F.3d 1342.

Vihul L., Czosseck C., Ziolkowski K., Aasmann L., Ivanov I.A., Brüggemann S., Legal Implications of Countering Botnets. Tallinn: NATO CCDCOE and ENISA Joint Report, Available at: https://ccdcoe.org/uploads/2012/03/VihulCzosseckZiolikowskiAasmannIvanovBruggemann2012_LegalImplicationsOfCounteringBotnets.pdf.

Walden I., Sentencing data-driven cybercrime: how UK courts tackle crime with cascading effects, „Computer Law and Security Review" 2024, no. 55(4).

Wired (2025) FBI investigates cryptocurrency pump and dump schemes. Available at: https://www.wired.com/story/fbi-cryptocurrency-pump-and-dump.