KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Bozhena Kozek

Criminal Law Protection of Critical Infrastructure against Computer Sabotage: A Ukrainian–German Comparative Analysis

Strafrechtlicher Schutz kritischer Infrastruktur vor Computersabotage: Eine deutsch-ukrainische Vergleichsanalyse

Betreuer:in/ Korrektor:in: Ass. Toma Mariana; Prof. Dr. Pierre Hauck, Dr. Schneider
YFC Chernivtsi / Justus-Liebig-Universität Gießen
Abgabedatum: 12.06.2026

Inhaltsverzeichnis

I. Introduction to the Topic 27
1. Relevance of the Study 27
2. The Concept of Computer Sabotage 27
3. The Concept of Critical Infrastructure 27
4. Aims, Objectives, and Methodology of the Study 28
II. Criminal Law Protection of Critical Infrastructure against Computer Sabotage in Ukraine 28
1. Legislative Framework 28
2. Elements of the Offence under Article 361 CCU 29
3. Challenges in Law Enforcement 29
4. Legislative Reform under the Influence of European Integration 30
III. Criminal Law Protection of Critical Infrastructure against Computer Sabotage in Germany 30
1. The Normative Framework: §§ 303a, 303b dStGB 30
2. Systemic Placement and Interaction with Administrative Law 31
3. Legislative Reform in Response to Contemporary Challenges 32
4. Judicial Practice and Doctrinal Debate 32
IV. Comparative Analysis and Conclusions 33
1. Comparative Characteristics of the Legal Regulation Systems 33
a) Architecture of Criminal-Law Regulation 33
b) Comparison of the Elements of the Offences (Article 361 CCU vs § 303b dStGB) 33
c) Approaches to Defining "Critical Infrastructure" – List-Based vs Evaluative 34
d) Comparison of Sanctioning Systems 34
e) Interaction between Criminal and Administrative (Regulatory) Law 35
2. Common Features and Fundamental Differences 35
3. Reasons for the Divergence 35
4. Assessment of Effectiveness with Empirical Data 36
V. Recommendations and Conclusions 37

I. Introduction to the Topic

1. Relevance of the Study

Example 1 (Ukraine): On 12 December 2023, Ukraine's largest mobile network operator "Kyivstar" was struck by what is widely considered the most destructive cyberattack against telecommunications infrastructure in European history. More than 24 million subscribers lost mobile and internet services for nearly two days, ATMs and payment terminals stopped functioning, and – most dangerously – the early-warning system of air-raid sirens was rendered partially inoperative in the midst of an active armed conflict. The Security Service of Ukraine attributed the attack to the "Sandworm" group, linked to the Russian military intelligence service (GRU). The incident was registered as criminal proceedings under Article 361 of the CCU.[1]

Example 2 (Germany): On 8 October 2022, two pairs of fibre-optic cables critical for the GSM-R communication system of Deutsche Bahn were deliberately severed at two distinct locations in Northern Germany. Within minutes, all long-distance and regional rail traffic between Berlin and the North Sea coast came to a halt; more than three million passenger journeys were affected. The Generalbundesanwalt opened proceedings on suspicion of computer sabotage and serious interference with public services. In the legal literature, the qualification was debated between § 303b dStGB (Computersabotage) and § 316b dStGB (Disruption of Public Services).[2]

The two examples illustrate two points. First, modern critical infrastructure (CI) is exposed to attacks that can do as much harm to public services and to national security as conventional sabotage. Second, the criminal-law qualification of these attacks is still unsettled, especially in armed conflict, when cybercrime, sabotage and war crime can overlap. The empirical side of the problem is discussed in IV.4.

2. The Concept of Computer Sabotage

In German doctrine, *Computersabotage* (§ 303b dStGB) denotes conduct that significantly disrupts the data processing of another. The functional equivalent in Ukrainian law is Article 361 CCU – *"несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем"* / "unauthorised interference with the operation of information, electronic communication and information-and-communication systems". Both norms protect the *integrity* of data and the *availability* of IT systems and must be distinguished from offences protecting data *confidentiality* (§ 202a dStGB, *Ausspähen von Daten*). The systemic implications of this distinction are explored in III.2. and IV.

3. The Concept of Critical Infrastructure

The contemporary EU framework rests on two pillars – Directive (EU) 2022/2557 on the resilience of critical entities (CER) and Directive (EU) 2022/2555 on a high common level of cybersecurity (NIS2)[3] – complemented by the Council of Europe Convention on Cybercrime (Budapest, 23.11.2001), to which both Germany and Ukraine

[1] On the Kyivstar attack of 12.12.2023 see the official statement of the Security Service of Ukraine of 04.01.2024, ssu.gov.ua; for the criminal-law qualification under Art. 361 CCU see Karchevskyi M., "Кібератаки на об'єкти критичної інфраструктури" [Cyberattacks on Critical Infrastructure Objects], *Інформаційне право* № 1/2024.

[2] "Strafbarkeit der Sabotage des Bahnverkehrs", *Legal Tribune Online* (lto.de), 9 October 2022; Bundesanwaltschaft, press release of 8 October 2022; on the substantive criminal-law qualification cf. Hilgendorf E., "Computersabotage und Verkehrsdelikte – zur Strafbarkeit der Bahnsabotage vom Oktober 2022", *JuS* 2023, p. 105 ff.

[3] Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities, OJ L 333, 27.12.2022, p. 164; Directive (EU) 2022/2555 of 14 December 2022 (NIS2), OJ L 333, 27.12.2022, p. 80.

are parties.[4] Germany operationalizes the concept through *Kritische Infrastrukturen* (KRITIS) and, in criminal law, through the open-textured criterion *"von wesentlicher Bedeutung"* in § 303b(2) dStGB – to be assessed by the court *in concreto*. Ukraine, by contrast, follows a list-based model under the Law of Ukraine "On Critical Infrastructure" No. 1882-IX of 16.11.2021.[5] The legal *technique* of identification differs fundamentally, with consequences explored in IV.

4. Aims, Objectives, and Methodology of the Study

This paper subjects the German and Ukrainian regimes to a *functional comparative analysis* – comparing the two legal orders by reference to the social problem each addresses rather than by surface terminology – (Zweigert/Kötz),[6] supplemented by *Rechtsdogmatik* and statistical analysis, within the theoretical framework of the German *Rechtsgutstheorie*.[7] Under the *Rechtsgutstheorie*, conduct may be criminalised only to the extent that it protects a *Rechtsgut* – a legal interest whose protection justifies the use of a criminal sanction.[8] Ukrainian doctrine has no direct equivalent; a similar role is played by the theory of the object of the offence (*теорія об'єкта злочину*): the object is the system of protected social relations (*суспільні відносини*) that the offence harms, and it is the social danger (*суспільна небезпека*) of the act to those relations that – under Articles 1 and 11 of the CCU – justifies its criminalisation.[9] The reasons for, and the consequences of, this difference are discussed in IV.3. II. sets out the Ukrainian regime, III. the German regime; IV. then makes the comparison (IV.1.–IV.2.), explains the doctrinal, legislative and cultural roots of the divergence (IV.3.), discusses effectiveness based on empirical data (IV.4.) and puts forward proposals for reform (IV.5.).

II. Criminal Law Protection of Critical Infrastructure against Computer Sabotage in Ukraine

1. Legislative Framework

The Ukrainian regime rests on Chapter XVI of the Special Part of the CCU – *"Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку"* [Criminal Offences in the Sphere of the Use of Electronic Computing Machines, Systems and Networks]. Three provisions are central: Article 361 CCU (unauthorised interference with the operation of information, electronic communication and information-and-communication systems), Article 361-1 CCU (creation, distribution and sale of malicious software or hardware), and Article 362 CCU (unauthorised actions with information by an insider).[10] Their construction – objective and subjective elements, including the requirement of intent (direct or, in some cases, indirect / *dolus eventualis*) – is set out in II.2.; the comparison with the German *Tatbestand* structure is taken up in IV.1.b).

4 Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS No. 185.
5 Закон України "Про критичну інфраструктуру" [Law of Ukraine "On Critical Infrastructure"] № 1882-IX від 16.11.2021, ст. 8.
6 Zweigert K. / Kötz H., *Einführung in die Rechtsvergleichung*, 3. Aufl. 1996, § 3 (functional comparative method); cf. Хавронюк М. І., *Кримінальне право зарубіжних країн* [Criminal Law of Foreign Countries], Київ 2024.
7 On *Rechtsgutstheorie* see Roxin C., *Strafrecht Allgemeiner Teil*, Band I, 4. Aufl. 2006, § 2 Rn. 1 ff.; in Ukrainian doctrine Тацій В. Я., *Об'єкт і предмет злочину в кримінальному праві* [Object and Subject of the Crime in Criminal Law], Харків 2016.
8 On the *Rechtsgutstheorie* as the dominant theory of legitimate criminalisation in German doctrine see Roxin, *Strafrecht Allgemeiner Teil I* (4th ed. 2006), § 2; M. D. Dubber, "Theories of Crime and Punishment in German Criminal Law", 53 *American Journal of Comparative Law* (2005) 679; T. Hörnle, "Rechtsgut and the Harm Principle", in Dubber/Hörnle (eds.), *The Oxford Handbook of Criminal Law* (2014).
9 On the theory of the object of the offence as protected social relations see Тацій, *Об'єкт і предмет злочину в кримінальному праві* [Object and Subject of the Crime in Criminal Law] (Kharkiv 2016); on the social danger (*суспільна небезпека*) of the act as the material feature of a criminal offence and the protective task of criminal law see Articles 11 and 1 of the CCU respectively.
10 Кримінальний кодекс України [Criminal Code of Ukraine] № 2341-III від 05.04.2001, Розділ XVI Особливої частини, статті 361, 361-1, 362, 363, 363-1, zakon.rada.gov.ua/laws/show/2341-14.

Specialised legislation supplements the Code: the Law of Ukraine *"Про критичну інфраструктуру"* [On Critical Infrastructure] No. 1882-IX of 16.11.2021 – adopting a *list-based* model of identification – and the Law *"Про основні засади забезпечення кібербезпеки України"* [On the Basic Principles of Cybersecurity of Ukraine] No. 2163-VIII of 05.10.2017, which establishes the institutional architecture (CERT-UA, the State Service of Special Communications, the NCCC under the NSDC).[11] Resolution of the Cabinet of Ministers No. 1109 of 09.10.2020 enumerates 25 sectors of critical infrastructure – energy, digital technologies, transport, healthcare, financial services, civil defence, defence-industrial complex, justice and others.[12]

2. Elements of the Offence under Article 361 CCU

According to Karchevskyi, the *generic object* (*родовий об'єкт*) of Chapter XVI offences is the cluster of "informational social relations the means of realisation of which are electronic computing machines, automated systems, computer networks and electronic communication networks".[13] The *direct object* of Article 361 CCU is the relations of property over computer information, complemented after the 2003–2004 amendments by an alternative direct object – the relations of provision and receipt of electronic communication services.[14]

In contrast to the German tradition (where the Bundesgerichtshof (BGH) and academic *Kommentare* have a strongly constitutive role), the elements of the Ukrainian offence are defined primarily by the *legislator*, as the literature consistently emphasises[15] – a feature whose comparative implications are developed in IV. The *objective side* (*об'єктивна сторона*) of Article 361 covers the act of unauthorised interference; its consequences are exhaustively enumerated: *leakage, loss, falsification, blocking of information, distortion of the process of its processing, and breach of the established order of its routing*.[16] The *subject* is general; the *subjective side* is intent (direct or indirect).[17]

The 2022 amendments introduced into Article 361 CCU a *qualified form* directed at critical infrastructure: the same act, if committed against an object of CI, is punishable by ten to fifteen years' imprisonment with confiscation of property – a sanction comparable to § 303b(4) dStGB; the comparative consequences are analysed in IV.1.d).[18]

A distinctive Ukrainian feature is ***Article 361-1 CCU*** (creation, distribution or sale of malicious software or hardware with the purpose of unauthorised interference) – a *formal corpus delicti* completed by the very act of creating or distributing such tools.[19] It is the functional equivalent of § 202c dStGB ("hacker tools") and constitutes one of the points where the Ukrainian-German comparison yields new findings (developed in IV.5.).

3. Challenges in Law Enforcement

Ukrainian practice faces a unique structural difficulty: the *delimitation of computer-sabotage offences from war*

[11] Закон України "Про основні засади забезпечення кібербезпеки України" [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine"] № 2163-VIII від 05.10.2017, ст. 1, 8.
[12] Постанова Кабінету Міністрів України № 1109 від 09.10.2020; Пашнєв Д. В. / Черевко К. О., *Вісник Кримінологічної асоціації України* 2024, № 1 (31), с. 209, 213–214.
[13] Карчевський М. В. [Karchevskyi M. V.], *Кримінально-правова охорона інформаційної безпеки України* [Criminal-Legal Protection of Information Security of Ukraine], Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2010, с. 105.
[14] Karchevskyi M. V., op. cit., с. 113–115.
[15] Тацій В. Я., "Об'єкт злочину" ["The Object of Crime"], *Вісник Асоціації кримінального права України* [Bulletin of the Association of Criminal Law of Ukraine] 2013, № 1(1), с. 126–143; Дудоров О. О. / Хавронюк М. І., *Кримінальне право. Навчальний посібник* [Criminal Law. Textbook], Київ: Ваіте, 2014.
[16] Стаття 361(1) КК України; Karchevskyi M. V., op. cit., с. 117–130.
[17] Karchevskyi M. V., op. cit., с. 132–133.
[18] Стаття 361(5) КК України в редакції 2022 р., прийнятій у зв'язку з введенням воєнного стану; пор. Pashnev / Cherevko, op. cit., с. 215.
[19] Karchevskyi M. V., op. cit., с. 133–138.

crimes and sabotage proper (Article 113 CCU, *диверсія / sabotage*; Article 438 CCU, *порушення законів та звичаїв війни / violation of laws and customs of war*). When a state-sponsored cyberactor attacks Ukrainian critical infrastructure during armed conflict, the prosecutor must choose between qualifying the act under Article 361 (cybercrime), Article 113 (sabotage), or Article 438 (war crime).[20] Since 2022 the Office of the Prosecutor General has registered all three qualifications in parallel proceedings, and in June 2024 prosecutors of the International Criminal Court (ICC) formally announced the investigation of Russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes.[21]

Returning to Example 1 from the Introduction, the December 2023 attack on Kyivstar illustrates this dilemma in concentrated form: registered under Article 361(5) CCU and, in parallel, referred by the SBU to the ICC Prosecutor under Article 438 CCU – a structural choice between cybercrime, sabotage and war-crime regimes that Ukrainian doctrine had hardly contemplated before 2022.[22] [23]

In case No. 735/739/20 of 19 September 2024, the Cassation Criminal Court of the Supreme Court of Ukraine confirmed that the post-2022 reformulation of Article 361 CCU does *not* decriminalise prior conduct: the new statutory term *"інформаційна (автоматизована) система"* / *"information (automated) system"* is broader and encompasses the previously used term *"комп'ютер"* / *"computer"* as a subtype.[24]

4. Legislative Reform under the Influence of European Integration

Ukraine's obligations under Article 9 of the EU-Ukraine Association Agreement and the Cybersecurity Strategy of Ukraine (Decree of the President No. 447/2021 of 26.08.2021) require continuous harmonisation with the contemporary EU framework – Directives (EU) 2022/2555 (NIS2) and 2022/2557 (CER).[25] Legislative initiatives registered in the Verkhovna Rada in 2023–2025 propose an evaluative criterion analogous to the German *"von wesentlicher Bedeutung"*, the expansion of Article 361-1 CCU to cover zero-day vulnerabilities, and a sectoral coordination mechanism functionally equivalent to the German Bundesamt für Sicherheit in der Informationstechnik (BSI). The concrete content of these proposals is analysed in IV.5.

III. Criminal Law Protection of Critical Infrastructure against Computer Sabotage in Germany

1. The Normative Framework: §§ 303a, 303b dStGB

The German regime rests on two tightly drafted dStGB provisions – § 303a (*Datenveränderung* / Data Alteration) and § 303b (*Computersabotage*). Both were introduced by the Second Act on Combating Economic Crime of 1986, substantially reformed by the 41st Criminal Law Amendment Act of 7 August 2007 in transposition of

20 Статті 113 (*Диверсія* / Sabotage), 438 (*Порушення законів та звичаїв війни* / Violation of Laws and Customs of War) КК України.

21 Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України [National Cybersecurity Coordination Centre at the NSDC of Ukraine], *Річний аналітичний огляд: жовтень 2023 – вересень 2024* [Annual Analytical Review: October 2023 – September 2024], с. 24, 29.

22 Ibid., с. 24.

23 Герасименко О. М. [Herasymenko O. M.], "Критична інфраструктура України як предмет наукового пізнання: теоретичний аспект" ["Critical Infrastructure of Ukraine as a Subject of Scientific Knowledge: Theoretical Aspect"], *Науковий вісник Ужгородського національного університету. Серія Право* [Academic Bulletin of Uzhhorod National University. Law Series] 2024, вип. 85, ч. 4, с. 42–45.

24 Постанова Касаційного кримінального суду Верховного Суду України від 19.09.2024 у справі № 735/739/20, провадження № 51-2737км23 [Decision of the Cassation Criminal Court of the Supreme Court of Ukraine of 19.09.2024, case No. 735/739/20]; reyestr.court.gov.ua/Review/121847592. For first-instance practice cf., e.g., вирок у справі № 397/1473/24 (unauthorised access to a banking information system).

25 Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [EU–Ukraine Association Agreement], ст. 9; Указ Президента України № 447/2021 від 26.08.2021 "Про рішення Ради національної безпеки і оборони України від 14.05.2021 'Про Стратегію кібербезпеки України'" [Decree of the President of Ukraine No. 447/2021 of 26.08.2021].

Council Framework Decision 2005/222/JHA, and recently amended through the NIS2-Umsetzungsgesetz (2024).[26]

§ 303a dStGB criminalises the unauthorised deletion, suppression, rendering-unusable or alteration of another person's data, with imprisonment of up to two years or a fine; the attempt is punishable, and § 303a(3) refers to § 202c dStGB to extend criminalisation to preparatory acts ("hacker tools"). The protected *Rechtsgut* is – according to the prevailing academic view and the case-law of the Bundesgerichtshof – the **integrity of data** as a specialised property interest, anchored constitutionally in BVerfGE 120, 274 (the *fundamental right to confidentiality and integrity of information-technology systems*).[27]

§ 303b dStGB criminalises the *significant disturbance* of a data processing operation that is *of substantial importance* (*von wesentlicher Bedeutung*) for another person. The provision distinguishes three modes of commission (Abs. 1): (i) data alteration in the sense of § 303a; (ii) the entering or transmission of data with intent to cause disadvantage – the typical DDoS scenario; (iii) destruction, damage, rendering-unusable, removal or alteration of data-processing hardware. The qualified form (Abs. 2) applies where the affected data processing is that of a foreign business, undertaking or public authority – the *de facto* gateway for prosecution of attacks against critical-infrastructure operators. § 303b(4) introduces *Regelbeispiele* – statutorily designated example cases that, while not formally qualifying the offence, trigger an aggravated sentencing range when present – with a penalty range from six months to ten years' imprisonment, including in particular the *endangerment of the supply of the population with vital goods* (Nr. 3 Var. 1) and the *endangerment of the internal or external security of the Federal Republic* (Nr. 3 Var. 2). § 303b(5) extends criminalisation to preparatory acts via § 202c.[28]

2. Systemic Placement and Interaction with Administrative Law

Of particular systemic importance is the placement of these offences within the architecture of the dStGB. §§ 202a–c dStGB (*Ausspähen, Abfangen* and *Vorbereiten des Ausspähens und Abfangens von Daten*) are located in *Abschnitt Fünfzehn* (*Verletzung des persönlichen Lebens- und Geheimbereichs*) and protect the **confidentiality** of data (*Datengeheimnis*). §§ 303a–c dStGB sit in *Abschnitt Siebenundzwanzig* (*Sachbeschädigung*) and protect the **integrity** of data and the **availability** of IT systems. This systemic location determines the addressees of the norm, the locus of the protected *Rechtsgut*, and the structure of the sanction.[29]

The dStGB does not operate in isolation. The Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSIG), the *KRITIS-Dachgesetz* of 2024, the *IT-Sicherheitsgesetz 2.0* of 2021 and the NIS2UmsuCG of 2024 form a regulatory layer of obligations imposed on critical-infrastructure operators (registration, incident reporting, minimum security standards). This layer interacts with the criminal law through the *"von wesentlicher Bedeutung"* criterion of § 303b(2) and through the *Regelbeispiele* of Abs. 4, with the BSI as the central administrative authority and frequent source of expert opinions in criminal proceedings.[30]

---

[26] § 303a, § 303b dStGB; 41. StrÄndG v. 07.08.2007, BGBl. I S. 1786; Council Framework Decision 2005/222/JHA, OJ L 69, 16.03.2005, p. 67; NIS2UmsuCG, RegE BT-Drs. 20/13751 v. 22.07.2024.

[27] § 303a Abs. 1, 3 dStGB; BVerfGE 120, 274 (302 ff.) (*IT-Grundrecht*); BGH NStZ 2022, 43 (44); Hilgendorf, in: Lackner/Kühl/Heger, *dStGB*, 30. Aufl. 2023, § 303a Rn. 1; MK-Wieck-Noodt, § 303a Rn. 4.

[28] § 303b Abs. 1–5 dStGB; on Abs. 2 see MK-Wieck-Noodt, § 303b Rn. 22–23; on the *Regelbeispiele* NK-Kargl, § 303b Rn. 26–27.

[29] On the systemic placement of §§ 202a–c (*Abschnitt 15*) versus §§ 303a–c dStGB (*Abschnitt 27*) and the resulting difference of *Rechtsgüter* (*Datengeheimnis* vs *Datenintegrität / Verfügbarkeit*), see Eisele J., *Computer- und Medienstrafrecht*, 2. Aufl. 2023, § 4 Rn. 1 ff.; Schönke/Schröder–Hecker, *dStGB*, § 303a Rn. 1, § 303b Rn. 1.

[30] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG); KRITIS-Dachgesetz (2024); IT-Sicherheitsgesetz 2.0 v. 18.05.2021, BGBl. I S. 1122.

3. Legislative Reform in Response to Contemporary Challenges

The most significant recent development is the NIS2UmsuCG[31], expanding the catalogue of operators subject to reporting obligations and introducing a 24-hour duty to notify significant cyber incidents. The KRITIS-Dachgesetz transposes Directive (EU) 2022/2557 (CER), unifying the physical and cyber dimensions of critical-entity resilience.[32] In parallel, the Federal Ministry of Justice has tabled a Ministerial Draft Bill on the Modernisation of Computer Criminal Law (*Referentenentwurf zur Modernisierung des Computerstrafrechts*) proposing targeted amendments to §§ 202a–c and § 303a dStGB designed to protect legitimate IT-security research without weakening the criminal-law protection of data.[33]

4. Judicial Practice and Doctrinal Debate

Two strands of case law deserve emphasis. On the constitutional foundation, *BVerfGE 120, 274* recognised the *fundamental right to confidentiality and integrity of information-technology systems*, which the BGH treats as the anchor of §§ 303a, 303b dStGB. On the **substantive elements**, the BGH confirmed that § 303a protects data integrity as such and that the *"wesentliche Bedeutung"* criterion of § 303b(2) is fulfilled, in mass-ransomware deployments, where the disturbance is capable of disabling the central organisational functions of the affected entity. On the act of criminal conduct (*Tathandlung*) of DDoS attacks, the BGH and the Landgericht Düsseldorf have established that mass automated requests resulting in the unavailability of the targeted server fall under § 303b(1) Nr. 2 dStGB.[34]

Returning to Example 2 from the Introduction, the Deutsche Bahn fibre-optic sabotage of 8 October 2022 illustrates the practical operation of this regime. The deliberate cutting of the GSM-R cables and the resulting halt of all long-distance and regional rail traffic in Northern Germany was qualified, in the legal commentary, as a textbook application of § 303b(2) dStGB, with potential overlap with § 316b dStGB and, given the geopolitical context, with the criminal sanction relevant example, so-called *Regelbeispiel* of § 303b(4) Nr. 3 (endangerment of the internal or external security of the Federal Republic).[35]

A second illustration is the Bundestag-Hack of May 2015: hackers attributed by the *Bundesamt für Verfassungsschutz* (BfV) to the Russian GRU's Unit 26165 (APT28) exfiltrated ca. 16 GB of parliamentary data, including emails of MPs and Chancellor Merkel. The *Generalbundesanwalt* issued an arrest warrant against D. Badin in May 2020; the EU imposed targeted sanctions in October 2020. The act was qualified as § 202a dStGB (*Ausspähen*) in concurrence with § 303a dStGB – illustrating the systemic interaction between the two non-adjacent sections of the dStGB analysed in III.2.[36]

The German doctrinal debate focuses today on the relationship between important factor i.e. *"wesentliche Bedeutung"* and the administrative concept of critical inastructure, in German called *"kritische Infrastruktur"*; the limits of preparatory criminalisation under §§ 202c, 303a(3), 303b(5) dStGB; and the criminal-law treatment of

31 Government Draft (Regierungsentwurf) of 22 July 2024, BT-Drs. 20/13751.
32 KRITIS-Dachgesetz (2024), transposing Directive (EU) 2022/2557 (CER).
33 Referentenentwurf des Bundesministeriums der Justiz zur Modernisierung des Computerstrafrechts (RefE ComputerStrafR) – Änderung der §§ 202a, 202b, 202c, 303a dStGB.
34 BVerfGE 120, 274 (302 ff.); BGH NStZ 2022, 43 (44 f.); BGH NStZ 2017, 470; LG Düsseldorf MMR 2011, 624 mit Anm. Bär; cf. Wissenschaftliche Dienste des Deutschen Bundestages, *Die Strafbarkeit des "Hackings" – Rechtslage im internationalen Vergleich*, WD 7 - 3000 - 104/23, 23.04.2024.
35 Cf. supra, Footnote 2; Hilgendorf E., "Computersabotage und Verkehrsdelikte – zur Strafbarkeit der Bahnsabotage vom Oktober 2022", *JuS* 2023, p. 105 ff.
36 On the Bundestag-Hack of May 2015 and the indictment of Dmitry Badin (Unit 26165 / APT28), see Federal Foreign Office, press releases of 2020; Council Decision (CFSP) 2020/1537 of 22 October 2020, OJ L 351 I/1; on the criminal-law qualification under §§ 202a, 303a dStGB, see Eisele J., op. cit., § 4 Rn. 8–12, 25 ff.

state-sponsored attacks in armed conflict – a point of convergence with the Ukrainian agenda developed in IV.[37]

IV. Comparative Analysis and Conclusions

1. Comparative Characteristics of the Legal Regulation Systems

a) Architecture of Criminal-Law Regulation

The CCU concentrates the relevant offences in Chapter XVI of its Special Part – a self-standing chapter dedicated to "computer offences" as a unified generic object of protection.[38] The German dStGB, by contrast, distributes the same factual subject matter across two non-adjacent sections: *Abschnitt Fünfzehn* (offences against data confidentiality, §§ 202a–c) and *Abschnitt Siebenundzwanzig* (offences against data integrity and IT-system availability, §§ 303a–c).[39] This architectural difference has substantive consequences: the CCU's single-chapter approach expresses a *unified informational Rechtsgut*; the dStGB's split architecture expresses a *differentiated theory of Rechtsgüter*. The Ukrainian model protects data as a whole; the German model dissects the same reality into specialised legal interests, with the textual location of each offence already implying its dogmatic profile.[40] These architectural choices in turn track the divergent theoretical groundings of criminalisation sketched in I.4.: the German *Rechtsgutstheorie* disaggregates protection by isolating each *Rechtsgut* as a distinct legal interest, whereas the Ukrainian theory of the object of the offence aggregates protection around the cluster of *суспільні відносини* that a single chapter is meant to safeguard.

b) Comparison of the Elements of the Offences (Article 361 CCU vs § 303b dStGB)

Element	**Article 361 CCU**	**§ 303b dStGB**
Rechtsgut	Property over computer information; provision/receipt of communication services	Functional integrity of data processing of substantial importance
Objektiver Tatbestand	Unauthorised interference causing leakage, loss, falsification, blocking, distortion, breach of routing	(i) data alteration as in § 303a; (ii) entering/transmitting data with intent to cause disadvantage (DDoS); (iii) damaging hardware
Subjektiver Tatbestand	Intent (direct or indirect)	Intent; § 303b(1) Nr. 2 requires *Nachteilszufügungsabsicht*
Subject	General – natural person ≥ 16 years	General; insider also covered
Basic sanction	Fine to 3 years' imprisonment	Up to 3 years' imprisonment or fine
Qualified form (CI)	Art. 361(5): 10–15 years + confiscation	§ 303b(2): up to 5 years; § 303b(4) Nr. 3: up to 10 years

[37] See in particular Hilgendorf E., "Computersabotage und Verkehrsdelikte – zur Strafbarkeit der Bahnsabotage vom Oktober 2022", *JuS* 2023, 105; for further contributions to the German doctrinal debate see *NStZ*, *ZStW* and *KripoZ* 2023–2024, as well as the *KripoZ* database on §§ 303a, 303b dStGB (kripoz.de).
[38] Розділ XVI Особливої частини КК України, статті 361, 361-1, 362, 363, 363-1.
[39] Eisele J., *Computer- und Medienstrafrecht*, 2. Aufl. 2023, § 4 Rn. 1 ff.
[40] Карчевський М. В., op. cit., с. 105–115; cf. Тацій В. Я., op. cit., с. 126–143.

Element	Article 361 CCU	§ 303b dStGB
Preparatory acts	Art. 361-1 CCU – autonomous formal *corpus delicti*	§ 202c dStGB (referenced via § 303a(3) and § 303b(5))

Source: Own presentation, based on the CCU (Art. 361) and the German Criminal Code (§ 303b dStGB).

Three substantive differences emerge. **First**, the *definitional source*. In Germany, the elements ("data", *"wesentliche Bedeutung"*) are crystallised through case-law and academic comments in the legal commentaries, German *Kommentare*;[41] in Ukraine, they are defined primarily by the *legislator* through statutory definitions in special laws to which the CCU implicitly refers or below the provision itself, with doctrinal commentary then eventually sporadically interpreting these definitions.[42] **Second**, the *structural openness* of the offence: § 303b dStGB centres on a single open-textured criterion to be applied *in concreto*, whereas Article 361 CCU exhaustively enumerates the consequences and relies on a formal register – the German technique trades predictability for adaptability, the Ukrainian one does the opposite. **Third**, the *placement of preparatory criminalisation*: Article 361-1 CCU is an autonomous offence with its own *corpus delicti*, whereas § 202c dStGB is structurally subordinated via cross-reference – the Ukrainian solution gives somewhat the preparatory offence higher systemic visibility, the German one achieves lower visibility but greater integration from this point-of-view.[43]

c) Approaches to Defining "Critical Infrastructure" – List-Based vs Evaluative

Ukraine follows we can finally say, a *list-based (formal) model*, i.e., the legal qualifier 'object of critical infrastructure' under Article 361(5) CCU is anchored not in a flexible normative criterion but in a closed administrative register that determines, in formal terms, what counts as CI: the Law "On Critical Infrastructure" No. 1882-IX, supplemented by Resolution of the Cabinet of Ministers No. 1109 of 09.10.2020, identifies 25 sectors and assigns CI status through formal inclusion in a sectoral register; the status is then *imported* into criminal law via Article 361(5) CCU. Germany follows an *evaluative (substantive) model*: § 303b(2) dStGB does not refer to a register; protection turns on the open-textured criterion of substantial importance (*"von wesentlicher Bedeutung"*), assessed by the court in light of the actual significance of the data processing. The Ukrainian model offers *predictability*; the German model *flexibility and technological neutrality*. Both orders identify largely the same sectors, but the legal *technique* of identification differs fundamentally.[44]

d) Comparison of Sanctioning Systems

The basic sanctions are roughly equivalent (Article 361(1) CCU: fine to 3 years' imprisonment; § 303b(1) dStGB: up to 3 years or fine). The qualified forms diverge sharply: § 303b(4) Nr. 3 dStGB provides for up to 10 years' imprisonment; Article 361(5) CCU provides for *10 to 15 years' imprisonment with confiscation*. The Ukrainian basic-floor for the qualified form thus *exceeds* the maximum German ceiling of the same form – a gap that reflects both the war-time emergency and a structural Ukrainian commitment to severe sanctions for serious offences

41 Schönke/Schröder–Hecker, *dStGB*, § 303b Rn. 1–10; MK-Wieck-Noodt, § 303b Rn. 9, 22–23; NK-Kargl, § 303b Rn. 17 ff.; LK-Goeckenjan, § 303a Rn. 25–38.
42 Карчевський М. В., op. cit., с. 132–138; Дудоров О. О. / Хавронюк М. І., op. cit.; Тацій В. Я., op. cit., с. 138–143.
43 § 202c dStGB; Article 361-1 CCU; cf. Karchevskyi M. V., op. cit., с. 133–138; Eisele J., op. cit., § 4 Rn. 25 ff.
44 Пашнєв Д. В. / Черевко К. О., op. cit., с. 213–214 (enumeration of 25 sectors per Кабінет Міністрів України № 1109); on the German evaluative criterion MK-Wieck-Noodt, § 303b Rn. 9.

against the State. Whether this severity *deters* state-sponsored attackers operating from outside Ukrainian jurisdiction is a separate empirical question (analysed in IV.4.).[45]

e) Interaction between Criminal and Administrative (Regulatory) Law

The German criminal law operates within a *dense and unified* regulatory ecology: here especially the main laws and regulations such as "BSIG, KRITIS-Dachgesetz, IT-Sicherheitsgesetz 2.0, NIS2UmsuCG"; the BSI is the single central administrative regulator, source of expert opinions in criminal proceedings, and gatekeeper of cybersecurity standards.[46] The Ukrainian regulatory layer is functionally similar but *institutionally distributed* across CERT-UA, the SSSCIP, and the NCCC under the NSDC, without a single equivalent of the BSI. This institutional fragmentation is the most concrete operational difference between the two systems and is reflected in IV.5. below.[47]

2. Common Features and Fundamental Differences

The two systems share four core commitments: criminal-law protection of data integrity and IT-system availability; implementation of the Council of Europe Convention on Cybercrime[48]; alignment with the EU acquis (NIS2, CER); and a separate qualified form for attacks on critical infrastructure. The fundamental differences are well captured by **two** dimensions: (i) the *list-based versus evaluative* identification of CI – a difference in legal *technique* with cascading consequences for predictability, adaptability and the burden of proof; and (ii) the *placement of preparatory criminalisation* – autonomous (Art. 361-1 CCU) versus cross-referenced (§ 202c dStGB) – a difference in *systemic architecture* with consequences for the visibility of the prohibition and the proportionality of preparatory liability.[49]

3. Reasons for the Divergence

The differences between the two systems are not coincidental. They reflect three structural choices, the first of which is doctrinal. As set out in I.4., the German *Rechtsgutstheorie* treats criminalisation as legitimate only when it protects a distinct *Rechtsgut*: where each type of harm – confidentiality, integrity, availability – is treated as a distinct legal interest, the dStGB places each in its own offence and its own section, so §§ 202a–c sit in Abschnitt 15 (*Datengeheimnis*) and §§ 303a–c in Abschnitt 27 (*Datenintegrität, IT-Verfügbarkeit*). Ukrainian doctrine, by contrast, sees the object of the offence as the system of protected social relations (*суспільні відносини*), and the social danger (*суспільна небезпека*) of the act provides the material ground for criminalisation under Articles 1 and 11 CCU. This broader approach appears in Chapter XVI of the Special Part, which treats the informational sphere as a single legal interest and brings all computer-related offences together in one chapter.[50]
The second source of divergence is the legislative technique used by the two parliaments to turn doctrine into rules. The Bundestag legislates through open normative criteria – the *"von wesentlicher Bedeutung"* standard in

[45] Стаття 361(5) КК України; § 303b(4) Nr. 3 dStGB; on sanctions in armed-conflict context see Pashnev / Cherevko, op. cit., c. 215.
[46] See § 1 et seq. BSIG; KRITIS-Dachgesetz (2024); IT-Sicherheitsgesetz 2.0 v. 18.05.2021; NIS2UmsuCG, see as well RegE BT-Drs. 20/13751.
[47] Закон України № 2163-VIII від 05.10.2017; Указ Президента № 447/2021 від 26.08.2021; Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України, *Річний аналітичний огляд: жовтень 2023 – вересень 2024*, с. 24–26.
[48] See Council of Europe Convention on Cybercrime (Budapest, 23 November 2001), ETS No. 185.
[49] Cf. supra, IV.1.b) and IV.1.c).
[50] On the "*Rechtsgutstheorie*" and the Ukrainian theory of the object of the offence see supra I.4. and the footnotes there.

§ 303b(2) dStGB being the main example – and leaves their application to the BGH and to the academic *Kommentare*. This division of work between courts and academic commentary is typical of post-war German criminal law.[51] The Verkhovna Rada, by contrast, follows the post-Soviet civil-law tradition in which the legislator does most of the work itself. It lists the consequences of Article 361 CCU in full (leakage, loss, falsification, blocking, distortion and breach of the order of routing) and assigns the identification of critical infrastructure to a closed register of 25 sectors set by the Cabinet of Ministers, rather than to a normative criterion.[52] The result is a trade-off between flexibility (the German technique) and predictability (the Ukrainian one), and above all a choice about who shapes the criminal-law rule – the courts or the legislator.

Third, the two systems rest on different ideas of what cybersecurity protects. The German framework developed in peacetime and in conditions of economic stability. It treats *Computersabotage* as a disruption of normal business and infrastructure activity, to be punished in proportion to the economic and organisational harm caused. Even the qualified form under § 303b(4) Nr. 3 dStGB caps imprisonment at ten years and ties its severity to the supply of vital goods and the security of the Federal Republic.[53] The Ukrainian framework has been reshaped by the full-scale invasion of 2022. The same conduct can now be prosecuted in parallel as cybercrime (Article 361 CCU), sabotage (Article 113 CCU) or war crime (Article 438 CCU). The basic sentencing floor of Article 361(5) CCU (ten to fifteen years' imprisonment with confiscation), together with the regular referral of state-sponsored cyberattacks to the ICC, shows a view in which protecting critical infrastructure cannot be separated from protecting the State itself.[54]

The three explanations are connected. A doctrine that separates legal interests works well with a legislator that drafts in open standards, while a stable state can leave the courts to work out how those standards apply in specific cases. The Ukrainian combination of a broader doctrine, a more detailed legislative technique and a wartime security context produces, in turn, a system that is severe, predictable and centred on the State.

4. Assessment of Effectiveness with Empirical Data

Empirical data confirm the comparative diagnoses above. In Germany, the PKS records a *roughly threefold increase* in cases under §§ 303a, 303b dStGB between 2019 and 2023.[55] In Ukraine, between October 2023 and September 2024 the NCCC registered tens of thousands of cyber incidents, ca. 30 percent of which targeted critical-infrastructure objects; the Office of the Prosecutor General reports a manifold increase in proceedings under Articles 361, 361-1, 362 CCU compared with the pre-war period.[56]

The German system's strengths lie in doctrinal maturity because there are decades of refined BGH case-law and dense academic *Kommentare* on §§ 303a, 303b dStGB, by contrast with the still-consolidating Ukrainian doctrine on Article 361 CCU, the flexibility of the term important factor, in German *"von wesentlicher Bedeutung"* criterion, and coordination with the infrastructure protection laws, such as BSIG/KRITIS-Dachgesetz (the fundamental

---

51 Eisele J., *Computer- und Medienstrafrecht* (2. Aufl. 2023), § 4 Rn. 1 ff.; on the partnership of BGH and academic *Kommentare* in concretising the *"wesentliche Bedeutung"* criterion see Hilgendorf E., in: Lackner/Kühl/Heger, *StGB* (30. Aufl. 2023), § 303b Rn. 4.

52 Карчевський М. В., *Кримінально-правова охорона інформаційної безпеки України* (Луганськ 2010); Хавронюк М. І., *Кримінальне право зарубіжних країн* (Київ 2024), on Ukrainian legislative technique; cf. Resolution of the Cabinet of Ministers of Ukraine No. 1109 of 09.10.2020 (catalogue of 25 sectors of critical infrastructure).

53 Hilgendorf E., "Computersabotage und Verkehrsdelikte – zur Strafbarkeit der Bahnsabotage vom Oktober 2022", *JuS* 2023, 105; Bundeskriminalamt, *Polizeiliche Kriminalstatistik (PKS) 2019–2023, Bundeslagebild Cybercrime* (bka.de).

54 Пашнєв Д. В. / Черевко К. О., "*Кібератаки на об'єкти критичної інфраструктури в умовах ведення війни: ключові поняття*", Вісник Кримінологічної асоціації України 2024, № 1(31), с. 209 ff.; cf. Office of the Prosecutor General of Ukraine, statistics on offences under Chapter XVI CCU (gp.gov.ua), and CERT-UA, "*Огляд кіберактивності проти України 2022–2024*" (cert.gov.ua).

55 Bundeskriminalamt, *Polizeiliche Kriminalstatistik (PKS) 2019–2023* – Bundeslagebild Cybercrime, Tab. T62 ("Datenveränderung, Computersabotage – §§ 303a, 303b dStGB"), bka.de.

56 НКЦК при Раді національної безпеки і оборони України, *Річний аналітичний огляд: жовтень 2023 – вересень 2024*, с. 24–26, 29; Офіс Генерального прокурора України, статистика за Розділом XVI КК України, gp.gov.ua.

infrastructure laws); its weaknesses, in complexity of application and limited deterrent effect on state-sponsored attackers. The Ukrainian system's strengths lie in the clarity of the list-based approach and rapid legislative adaptation – still or even - in wartime; its weaknesses, in limited judicial practice, the cybercrime/sabotage/war-crime trilemma and institutional fragmentation.[57]

V. Recommendations and Conclusions

Therefore, the comparative analysis suggests four short proposals for Ukrainian legislative development drawing on German experience and EU integration.

First, introduce, alongside the existing register-based identification of CI, an *evaluative criterion* analogous to § 303b(2) dStGB to enable courts to qualify attacks on objects not yet registered.

Second, preserve and strengthen Article 361-1 CCU as an autonomous preparatory offence – extending it to cover the procurement of zero-day vulnerabilities, in alignment with the Federal Ministry of Justice's Ministerial Draft Bill on the Modernisation of Computer Criminal Law (*Referentenentwurf zur Modernisierung des Computerstrafrechts*).

Third, develop a single sectoral coordination mechanism analogous to the BSI – between the SSSCIP, CERT-UA and the NCCC – to consolidate institutional fragmentation.

Fourth, develop *judicial guidelines* for the qualification of cyberattacks in armed conflict, distinguishing Art. 361, Art. 113 and Art. 438 CCU – a question on which Ukrainian doctrine and practice have advanced significantly since 2022.[58]
Conversely, the Ukrainian experience offers Germany two lessons: the autonomous preparatory offence (Art. 361-1 CCU) and the explicit war-crime track (Art. 438 CCU) for state-sponsored cyberattacks in armed conflict.

Neither system, on its own, meets all the demands of modern cybersecurity. The German system offers careful doctrine and a unified regulatory framework. The Ukrainian system offers a clear list-based identification of critical infrastructure and an independent preparatory offence under Article 361-1 CCU.

European law – above all the NIS2 Directive, the CER Directive and the EU–Ukraine Association Agreement – is bringing both systems closer to a common model that combines formal registers with normative criteria. The comparison made above suggests that this convergence should not be left to European harmonisation alone, but developed in a deliberate way, with each system learning from the other.

[57] Cf. supra, Examples 1 and 2 of the Introduction (I.1.) and II.3.
[58] Referentenentwurf des Bundesministeriums der Justiz zur Modernisierung des Computerstrafrechts; Articles 113, 438 КК України; cf. Карчевський М. В., op. cit., с. 133–138 (on Art. 361-1 CCU as autonomous preparatory offence).

Bibliography / References

Borysov V. I., Karchevskyi M. V., Shepitko M. V. (eds.). Mizhnarodni standarty ta natsionalna kryminalno-pravova polityka u sferi zakhystu informatsiinoi bezpeky [International Standards and National Criminal-Law Policy in the Sphere of Information Security Protection]. Харків. 2023.

Dudorov O. O., Khavroniuk M. I. Kryminalne pravo. Navchalnyi posibnyk [Criminal Law. Textbook]. Київ. 2014.

Eisele J. Computer- und Medienstrafrecht. 2. Aufl. 2023.

Gutorova N. Strafrechtliche Folgen der Geldwäsche in der Ukraine und ihre Übereinstimmung mit Acquis Communautaire. Ost/Letter. 2023. No. 1.

Herasymenko O. M. Krytychna infrastruktura Ukrainy yak predmet naukovoho piznannia [Critical Infrastructure of Ukraine as a Subject of Scientific Knowledge]. Науковий вісник Ужгородського національного університету. Серія Право. 2024. Вип. 85. Ч. 4. С. 42–47.

Hilgendorf E. Computersabotage und Verkehrsdelikte – zur Strafbarkeit der Bahnsabotage vom Oktober 2022. JuS. 2023. S. 105 ff.

Karchevskyi M. V. Kryminalno-pravova okhorona informatsiinoi bezpeky Ukrainy [Criminal-Legal Protection of Information Security of Ukraine]. Луганськ. 2010.

Khavroniuk M. I. Kryminalne pravo zarubizhnykh krain [Criminal Law of Foreign Countries]. Київ. 2024.

Lackner/Kühl/Heger (eds.). StGB. 30. Aufl. 2023 (cited as: Lackner/Kühl/Heger-author, § …).

Leipziger Kommentar zum StGB (cited as: LK-author, § …).

Münchener Kommentar zum StGB (cited as: MK-author, § …).

Nomos Kommentar zum StGB (cited as: NK-author, § …).

Pashniev D. V., Cherevko K. O. Kiberataky na obiekty krytychnoi infrastruktury v umovakh vedennia viiny: kliuchovi poniattia [Cyberattacks on Critical Infrastructure in Time of War: Key Concepts]. Вісник Кримінологічної асоціації України. 2024. No. 1 (31). С. 209 ff.

Roxin C. Strafrecht Allgemeiner Teil. Band I. 4. Aufl. 2006.

Schönke/Schröder (eds.). StGB. 30. Aufl. 2019 (cited as: Schönke/Schröder-author, § …).

Tatsii V. Ya. Obiekt zlochynu [The Object of Crime]. Вісник Асоціації кримінального права України. 2013. No. 1 (1). С. 126–143.

ders. Obiekt i predmet zlochynu v kryminalnomu pravi [Object and Subject of the Crime in Criminal Law]. Харків. 2016.

Zweigert K., Kötz H. Einführung in die Rechtsvergleichung. 3. Aufl. 1996.

Die Kriminalpolitische Zeitschrift (KriPoZ) darf dieses Werk unter den Bedingungen der Digital Peer Publishing Lizenz (DPPL) elektronisch übermitteln und zum Download bereitstellen. Der Lizenztext ist im Internet abrufbar unter der Adresse http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-de0.