



International Journal of Cyber Law

Legal Limits of Active Cyber Countermeasures by Private Corporations

Tiberio Graziani^{1*}

¹ International Institute for Global Strategic Analysis (IIGSA)

* tibgraziani@gmail.com

ABSTRACT

Private corporations increasingly face cyber attacks yet lack clear legal authority to respond. International law grants states self-defense rights but offers no equivalent protection for firms. Italian law, particularly Article 615-ter of the Criminal Code, criminalizes unauthorized access without exception for defensive intent. This creates a gap between corporate technical capability and legal permission. This study aims to examine existing legal limits, identify boundaries between lawful defense and unlawful retaliation, and propose clearer standards for corporate conduct. Using a qualitative, doctrinal approach combined with document analysis, the research examined statutes, European directives, and peer-reviewed legal scholarship. Results show international law provides no defensive right, current statutes ignore intent and proportionality, and a narrow amendment could responsibly close this gap. The study recommends precise legislative drafting, mandatory oversight, sector-specific rules, judicial training, and international cooperation. These findings offer a practical path toward balanced, accountable private cyber defense across evolving digital legal systems.

Keywords: *Private Cyber Defense, Active Cyber Countermeasures, Article 615-ter, Italian Criminal Law, Cyber security Regulation, Proportionality and Necessity, Corporate Liability*

HOW TO CITE THIS ARTICLE (APA 7th Edition)

Graziani, T. (2026). Legal Limits of Active Cyber Countermeasures by Private Corporations. *International Journal of Cyber Law*, 1(2), 45–59. <https://doi.org/10.59022/IRSHAD-ijcl.16>

I. INTRODUCTION

Private companies now face cyber attacks that public defense cannot fully stop. Many firms consider striking back instead of only defending their networks. This method is called active cyber defense, sometimes named hacking back. It raises hard legal questions about corporate power and state authority. Should private firms hold the right to strike attackers directly? International law was built mainly for states, not corporations. Courts and regulators still lack settled rules for corporate countermeasures. This gap creates real risk for businesses acting without legal guidance. Legal scholars now debate where private cyber defense must stop. This paper studies the legal limits placed on corporate active countermeasures. It explores how far private entities may lawfully act in cyberspace. Careful limits matter because one mistake can trigger wider conflict. This topic sits at the center of modern cyber security law today. Corporations therefore need clear, settled legal answers before acting under pressure (Denning, 2014).

Cyber security threats have grown faster than the legal rules meant to control them. Governments traditionally held the main right to respond to armed attacks. Private corporations were never given equal authority under this old framework. Yet many companies now possess the technical skill to strike back. Firms often feel abandoned when public agencies respond too slowly. This has pushed some corporations toward unauthorized retaliatory action online. Legal systems worldwide have not kept pace with this practical shift. Few countries offer clear statutes governing private cyber retaliation today. Existing laws focus heavily on banning unauthorized access to computer systems. They rarely explain when limited self-defense might become justified. This leaves confusion for corporate security teams and legal advisors alike. Cross-border data rules add further complexity to private response options. The current legal landscape remains fragmented across many jurisdictions. This background sets the stage for examining private countermeasures more closely (Cook, 2018).

Active cyber defense currently carries significant legal uncertainty for private firms. Companies often act without clear boundaries or established internal procedures. Current cybercrime laws generally criminalize unauthorized access to computer systems. This ban includes access aimed at stopping an ongoing attack. Legislative frameworks have not evolved to cover corporate self-defense options. This research examines exactly where legal boundaries currently sit today. It identifies which specific countermeasures might be permissible under existing law. We still need clarity on acceptable proportionality and necessary restraint levels. Questions remain about liability when countermeasures cause unintended third-party damage. This study addresses these unresolved questions directly and systematically. It aims to map the boundary between lawful defense and unlawful retaliation. Without clarity, corporations face unpredictable legal and financial exposure daily. No accepted framework currently guides these difficult corporate decisions in practice. This absence of clear guidance leaves firms exposed to serious ongoing legal risk (Barnes, 2018).

Scholars have long debated whether private entities deserve defensive cyber powers. Traditional legal views hold that only states may lawfully use force. Recent scholarship challenges this old assumption given growing corporate technical capacity. One recent study argues that private active defense increasingly overlaps with state security functions. This overlap creates tension between national security interests and corporate autonomy. This analysis pushes the debate toward hybrid governance models instead. It suggests some public oversight of private defense actions. This finding highlights how blurred these once-clear boundaries have truly become. Corporations now operate within a space once reserved strictly for states. Such overlap raises fresh questions about accountability when private action fails. Regulators still struggle to classify these hybrid defensive actions under existing statutes. This uncertainty pushes many firms toward cautious, purely defensive strategies instead. The trend nonetheless signals a slow but steady shift in public and private cyber roles (Broeders, 2021).

Other researchers focus on threat classification within tightly regulated industries. One recent study examined cyber threats specifically within the banking and financial sector. Their study categorized several countermeasure strategies used by financial institutions. They found that most countermeasures remained purely defensive in nature. Few firms pursued active retaliation despite having the technical capability to act. This restraint reflects real awareness of legal exposure and reputational risk. Their findings suggest industry self-regulation may often precede formal legislation. Together, these studies show growing scholarly attention toward private sector cyber roles. Both works highlight the widening gap between technical capability and legal permission. Neither study fully resolves how liability should be assigned after action. This missing piece leaves practitioners without firm practical guidance for decisions. Financial firms in particular must weigh reputational cost against defensive necessity carefully. Such tension continues shaping how corporations approach active cyber defense choices today (Darem et al., 2023).

Existing literature strongly addresses state responsibility and international cyber norms. However, few studies examine corporate legal liability for offensive countermeasures. Most research treats private and state actors as entirely separate categories. Few scholars analyze how domestic law might authorize limited corporate action. Suggestions for future research often call for clearer regulatory frameworks ahead. Yet detailed legal analysis of specific limits remains genuinely scarce today. This gap leaves corporations without predictable legal standards to follow closely. This study addresses that gap by mapping precise legal boundaries carefully. It focuses specifically on proportionality, necessity, and corporate accountability standards. New research should clarify when private countermeasures become legally acceptable. This paper contributes toward that necessary legal clarification for practitioners and courts. Filling this gap will help regulators draft

more workable future statutes. It will also give corporate counsel firmer ground for daily client advice. Courts too would benefit from a clearer legal standard (Gerke, 2021).

To examine existing legal frameworks governing private cyber countermeasures.

To identify the boundaries separating lawful defense from unlawful retaliation.

To propose clearer legal standards for corporate cyber defense conduct.

What legal limits should govern private corporations using active cyber countermeasures?

This research matters because legal uncertainty currently threatens corporate cyber security practice. Companies need clear guidance before deploying active defense measures. Without clarity, firms risk severe legal and diplomatic consequences. This study contributes new knowledge to an underdeveloped legal field. It offers practical guidance for lawmakers drafting future cyber security legislation. Legal practitioners will benefit from clearer standards when advising corporate clients. Policymakers gain a framework for balancing security needs with legal restraint. Academically, this research bridges international law and corporate cyber security practice. It strengthens ongoing scholarly conversations about private sector legal responsibility. Insurance providers may also use these standards to assess corporate cyber risk. Cross-border businesses gain from more predictable, harmonized legal expectations. Judges deciding future disputes will have firmer legal ground to rely on. Smaller firms without large legal teams particularly need this kind of clarity. The findings can therefore support fairer outcomes across firms of every size (Dziwisz, 2024).

II. METHODOLOGY

This research uses a qualitative research design built around legal analysis. Qualitative methods suit legal research because law relies on interpretation, not numbers. This approach lets the study examine meaning, intent, and legal reasoning closely. The population for this research is the wider body of cyber security law. This includes international, European, and domestic Italian legal frameworks together. From this broad population, the study samples one specific legal provision. That sample is Article 615-ter of the Italian Criminal Code itself. This provision governs unauthorized access to computer systems within Italy. The study also draws on related instruments, including the NIS2 Directive. It further considers the EU Cyber Resilience Act and comparable national statutes. Focusing on one statute allows detailed, in-depth legal examination within limited scope. This targeted sample keeps the research manageable while remaining analytically meaningful. The chosen sample directly reflects the research question guiding this entire study.

Data collection relied on carefully chosen keywords across academic and legal databases. Search terms included active cyber defense, hacking back, and private countermeasures. Other keywords included Article 615-ter, Italian cybercrime law, and cyber attribution. These keywords guided searches across journal databases and academic search platforms. Scholarly articles came primarily from peer-reviewed law and cyber security journals. Legal texts came directly from official government and institutional websites instead. The Italian Ministry of Justice website provided access to the current criminal code. The European Union's official legal portal supplied relevant directives and regulations. This combination of scholarly and official sources strengthened the overall evidence base. Official legal texts confirmed the exact current wording of relevant statutes. Scholarly articles provided interpretation, critique, and comparative legal perspective around them. Using both source types together supported a more complete legal analysis. This dual approach balanced authoritative legal text with expert academic commentary.

This research primarily used doctrinal analysis alongside broader document analysis techniques. Doctrinal analysis examines legal texts, principles, and their internal logical structure. Document analysis reviewed scholarly articles, official reports, and policy statements together. To ensure validity, only recent scholarly sources were used

wherever possible. Most cited articles were published within the last five years. The study also confirmed that cited laws remained currently applicable and unamended. This research relied solely on documents already available within the public domain. Every scholarly source used received a full and accurate citation throughout. This practice credits original authors and supports transparent, verifiable academic work. The researcher maintained no conflict of interest during this entire study. The study also acknowledges clear limitations tied to its evolving subject matter. Technology and cyber security policy change quickly, sometimes within a matter of months. Laws discussed here may therefore be amended again after this research concludes. This limitation reflects the inherently dynamic nature of digital and legal environments.

III. RESULTS

This research asked what legal limits should govern private active cyber defense. Corporations increasingly now possess the technical skill to strike back at attackers. Yet international and domestic law rarely address this growing capability. The study set three clear research objectives guiding this investigation from the start. It examined existing legal frameworks covering private cyber countermeasures. It also sought to identify the boundary between lawful defense and unlawful retaliation. Finally, it aimed to propose clearer legal standards for corporate conduct. These objectives directly shaped the central research question posed earlier. Answering that question required close analysis of international law, domestic statutes, and legal literature. The following results present what this analysis revealed. Each result connects directly to one of the stated research objectives above. Together, they build a clearer picture of an unsettled legal area. Policymakers, courts, and corporations all have a stake in these findings (Leventopoulos et al., 2024).

International law does not grant private corporations a right to self-defense. State responsibility rules apply mainly to governments, not private companies. A state may lawfully respond to an attack under strict conditions. Corporations hold no equivalent status under this traditional legal framework. This means firms cannot claim the same justification that states use. Private active cyber defense therefore lacks recognized international legal support today. Companies acting under this false assumption face real legal exposure abroad. Some corporations still believe technical capability grants implicit legal permission. This belief is mistaken and creates risk during cross-border incidents. International bodies have not extended self-defense doctrine to non-state actors. Existing treaties and customary rules stay silent on corporate cyber responses. This silence leaves companies without any settled legal basis for retaliation. Firms must therefore rely on domestic law for defensive guidance. Clear rules at the international level remain absent for private entities (Kello, 2021).

IV. DISCUSSION

Article 615-ter of the Italian Criminal Code punishes unauthorized access to computer systems. It protects systems secured by technical or organizational safeguards. The provision covers hackers, insiders, and outsiders who breach networks. It makes no distinction between an attacker and a defending firm. A company accessing an intruder's system still commits a crime. This holds even when the access aims only to stop an attack. Italian courts apply the article strictly, without room for defensive exceptions. This strict approach reflects the law's focus on preventing intrusion generally. It was never designed with corporate cyber defense in mind. Digital investigations increasingly reveal this gap between statute and practice. Prosecutors and defense counsel face growing uncertainty in borderline cases. Companies attempting limited defense risk full criminal liability under current wording. This rigid framework sits awkwardly beside rising cyber attack sophistication. Reform discussions in Italy have addressed this outdated gap (Flor & Panattoni, 2023).

The amendment's core purpose is closing this gap between law and practice. It aims to create a narrow, clearly defined defensive exception. This exception applies only when a company faces an active intrusion. The defender could act only within its own network's boundaries. Any action beyond that boundary stays fully criminal under the code. This narrow scope stops the amendment from becoming a license for retaliation. Lawmakers designed it to close a real gap, not a new one. Attribution problems make this scope especially important for drafters today. Identifying the true source of an attack often proves technically difficult. A wrongly targeted response could harm an innocent third party. The amendment therefore requires a reasonable, good-faith belief about the attack's origin. This requirement protects innocent parties from mistaken countermeasures. It also keeps the defending firm within a testable standard. Such careful drafting balances corporate need against public safety (Rid & Buchanan, 2015).

The proposed amendment sets strict conditions before any defensive action becomes lawful. A company must first show clear proof of an ongoing intrusion. Mere suspicion or late detection would not satisfy this standard. The response must also remain proportionate to the actual threat faced. Firms cannot use this defense to justify aggressive countermeasures. Necessity forms another core condition written into the proposed text. Companies must first try less intrusive defensive steps where possible. Only when those steps fail does active countermeasure become legally available. Time also matters heavily under this proposed framework. The defensive window closes once the intrusion itself has clearly ended. Acting after that point would fall outside the amendment's narrow protection. These conditions together prevent the exception from swallowing the general rule. Courts would still assess each case against this strict multi-part test. Such structured conditions keep corporate defense predictable and legally accountable (Sánchez-García et al., 2023).

Oversight forms a second pillar supporting the amendment's design. Any company using this defense faces mandatory reporting duties afterward. Reports would go directly to Italy's National Cyber security Agency for review. This agency, known as ACN, already coordinates national cyber incident response. Adding this reporting duty keeps corporate action within public view. It also builds a record for future policy and legal review. Judges would retain full power to review each defensive action taken. A company could not escape scrutiny simply by invoking the new provision. This judicial check balances corporate flexibility against the risk of misuse. Independent oversight prevents the exception from becoming a hidden shield. Regulators could also revoke recognition from firms that abuse the provision. Repeated or reckless use would trigger closer investigation and possible sanctions. This layered system builds public trust in the amended legal framework. Accountability therefore remains central to the amendment's legal design (Pietropaoli, 2024).

Any Italian reform must fit within EU cyber security law. The NIS2 Directive sets strict security duties for critical sectors. It requires firms to report incidents and strengthen internal cyber defenses. The proposed amendment complements these duties without weakening existing reporting obligations. Companies would still meet NIS2 requirements even while using limited defensive measures. The EU Cyber Resilience Act adds pressure toward stronger product security. Together these legal instruments push firms toward stronger cyber security management. Italy's amendment can align with this shift instead of standing apart from it. Harmonizing domestic and EU rules avoids conflicting duties for firms. It also positions Italy alongside other states debating similar reforms. Some European countries already discuss narrow private cyber defense. A coordinated European approach would reduce legal fragmentation across the market. Italy's proposal could therefore serve as one model within a wider debate. This alignment strengthens the amendment's legal and political viability (Kulesza, 2021).

Ethical concerns run alongside every legal question raised by this amendment. Critics worry private defense could shift firms from protection toward offense. A defender with legal cover might act beyond genuine necessity. This risk explains why the amendment keeps such narrow, testable boundaries. Supporters counter that doing nothing also carries real ethical costs. Victims left without any lawful defensive option may suffer repeated attacks. Waiting for slow state response can let serious harm continue unchecked. The amendment tries to balance these competing ethical concerns carefully. It grants limited power while keeping strict checks against clear misuse. This balance reflects wider debate about proper limits on private force. Ethics scholars stress private security must remain firmly rule-bound. Unchecked corporate power in cyberspace could become dangerous rather than protective. The amendment's conditions directly answer this ethical worry through legal structure. Good law must satisfy both practical need and moral caution (Pattison, 2020).

Italy has strengthened its national cyber security institutions and legal focus. The National Cyber security Agency plays a growing role in policy design. Lawmakers have shown interest in updating criminal provisions for digital threats. Rising ransom ware attacks against Italian firms have pushed this reform higher up the agenda. Public and private cooperation has also increased through joint response exercises. These developments create favorable conditions for a careful defensive exception. The proposed amendment fits naturally within this broader modernization effort. It offers a practical answer to a problem regulators already recognize. Passing this amendment would not weaken criminal protections for victims. Instead, it adds a narrow, closely supervised defensive option. This balance supports corporate resilience and continued public accountability. Italy could become an early example for other nations facing similar gaps. The reform reflects a broader shift toward risk-based cyber security law. Thoughtful legal reform can keep pace with fast-changing digital threats (Flor, 2025).

Current Article 615-ter treats every unauthorized access as a criminal act. It draws no line between an attacker and a responding victim. Any entry into a protected system triggers the same criminal charge today. Intent behind the access simply does not matter under the current wording. This blanket approach reflects the law's original goal of

stopping intrusion. The proposed amendment changes this picture in one important way. It carves out a narrow space where defensive access becomes lawful. That space applies only during an active, ongoing cyber intrusion. Outside that window, the original blanket rule still fully applies. This difference marks a shift from pure prohibition toward limited permission. Italian criminal law rarely grants such conditional exceptions for private actors. Comparative studies show similar rigidity across many cybercrime statutes. The amendment represents a notable departure from traditional legal design. It moves Italian law closer to conditional defensive permission (Fusco, 2020).

Current law also ignores intent entirely once unauthorized access is proven. A curious insider and a hostile attacker face identical criminal exposure. Courts need only show that access occurred without proper authorization. Motive plays no formal role in establishing criminal liability here. The proposed amendment changes this by placing intent at its center. It requires proof of a genuine defensive purpose behind the access. A defender must show real belief that an attack was actively occurring. This shifts the legal inquiry from pure access toward reasoned justification. Courts would need to examine evidence of the attacker's ongoing conduct. Comparative jurisprudence shows most cybercrime laws share this intent-blind structure. Few jurisdictions build a defensive-intent test into statutory text. This makes the Italian proposal unusual within broader legal practice. Such reform still fits within recognized doctrines of necessity and justification. The shift toward intent reflects a more nuanced legal approach (Zlati, 2024).

Current Article 615-ter includes no proportionality or necessity requirement. A single unauthorized entry triggers liability regardless of scale or intensity. The law treats a small probe the same as a serious breach. This uniform treatment leaves no room for measured, situation-specific judgment. The amendment introduces proportionality as a core legal requirement instead. A defensive response must match the seriousness of the actual threat. Excessive or disproportionate action would fall outside the amendment's protection entirely. Necessity also works alongside proportionality within this new legal structure. Companies must show that milder defensive options were tried or unavailable. This dual test did not exist anywhere within the original 1993 provision. Adding it brings Italian law closer to broader international legal standards. Many cyber security frameworks already stress the value of proportionate response. This shift signals a move toward more calibrated legal judgment. The change reflects growing global thinking on responsible cyber security practice (Chiara, 2024).

Current law imposes no reporting duty tied to unauthorized access itself. A firm accused under Article 615-ter simply faces standard criminal proceedings. There is no built-in mechanism connecting defensive action to national oversight. Prosecutors handle each case through ordinary criminal procedure alone. The amendment changes this by adding a mandatory reporting requirement. Companies using the defensive exception must notify the National Cyber security Agency. This creates a direct link between private defensive action and public oversight. Recent Italian cyber security legislation already pushes toward closer incident coordination. The DDL Cybersicurezza reform strengthens ties between investigation and incident response teams. The proposed amendment fits neatly within this broader coordination trend. It adds a specific reporting channel absent from current criminal provisions. This transparency requirement did not exist under the original statute. Such reporting also creates useful data for future policy evaluation. The change reflects a shift toward coordinated, monitored defensive practice (Fiorinelli, 2024).

Current Article 615-ter says nothing about protecting data belonging to third parties. A defender responding to an intrusion could accidentally expose personal data. Existing criminal provisions focus purely on access, not data handling. This silence creates real risk during any technical defensive response. The amendment addresses this gap by embedding data protection safeguards directly. Any permitted defensive action must still respect data protection by design. Companies cannot use this exception to justify careless data exposure. This requirement borrows from established European data protection principles. It ensures defensive tools stay narrowly targeted at the intruder. Broader network scanning or data collection would fall outside protection. This safeguard did not exist within the current statutory text. Its addition reflects growing legal attention to privacy during response. Modern cyber security law increasingly treats privacy and security as connected values. The amendment therefore blends criminal law with wider data protection principles (Jasmontaite et al., 2018).

Article 615-ter dates back to Italy's original 1993 computer crime reform. That reform focused mainly on stopping early digital intrusion. Lawmakers then had little reason to consider organized corporate cyber defense. Cyber threats at the time looked simple compared to modern attacks. The statute reflected that narrower, earlier understanding of digital risk. Decades of technological change have since outpaced this original legal design. Attackers now use automated tools and coordinated global infrastructure routinely. Companies also hold far greater technical capacity than before. Older privacy and computer crime laws already showed early signs of strain. Legal scholars long noted gaps between fast technology and slow legislation. The proposed amendment responds directly to this widening historical gap. It updates a statute never built for today's cyber environment. This evolution mirrors patterns seen

across many national legal systems. Modern reform continues a much older struggle between law and technology (Perri & Zanero, 2004).

Current Article 615-ter stays fixed while cyberspace keeps evolving quickly. It offers no built-in mechanism for future legal adjustment. Each new threat type requires separate legislative or judicial action. The proposed amendment instead builds in room for future refinement. Its reporting and oversight structure allows regulators to gather ongoing evidence. That evidence can later guide further updates to the legal framework. Recent Italian scholarship already explores how cyberspace challenges traditional legal categories. Debates continue over concepts like digital confidentiality and evolving privacy. These discussions suggest cyber law will keep changing well beyond this amendment. The amendment acts as one step within a longer legal journey. It does not claim to permanently solve every future cyber security question. Instead, it creates a flexible starting point for careful legal growth. This adaptable design differs sharply from the static original 1993 provision. The comparison shows how modern reform anticipates constant technological change (Meccariello, 2026).

Applying Article 615-ter often starts with a difficult attribution problem. Investigators must first prove who actually accessed the protected system. Skilled attackers frequently hide behind proxies, botnets, and rented foreign infrastructure. This makes tracing a real identity technically slow and uncertain. Weak attribution evidence can collapse an otherwise strong criminal case quickly. Prosecutors then struggle to meet the required standard of proof. Cross-border attacks add another layer of difficulty for investigators here. Servers and intermediaries often sit outside Italian legal jurisdiction entirely. Cooperation with foreign authorities can take many months or even years to complete. Meanwhile, digital evidence may disappear or lose its practical value entirely. Courts must weigh incomplete technical evidence against strict legal standards. This mismatch between technical uncertainty and legal certainty creates real strain. Scholars increasingly frame this as a deeper public-private security challenge. Effective enforcement therefore depends heavily on close international legal cooperation today (Thumfart, 2020).

A second challenge involves ethical hackers who test system security legally. Many researchers probe systems to find flaws before criminals do. Article 615-ter draws no clear line protecting this useful research activity. A researcher without explicit permission faces the same criminal charge. This creates a chilling effect on legitimate security testing work. Skilled researchers may avoid reporting flaws out of fear of prosecution. Companies lose valuable early warnings about weaknesses in their own systems. Some European scholars now call for stronger protection for these hackers. Clearer rules could separate malicious intrusion from genuine security research. Without protection, valuable expertise stays underused across the cyber security field. Prosecutors also face hard judgment calls when researchers act in good faith. Determining true intent behind an unauthorized test remains hard. This uncertainty complicates fair and consistent application of current law. Better clarity would benefit both researchers and enforcement authorities alike (Rampásek et al., 2026).

Penetration testing and bug bounty programs create another practical legal challenge. Companies now hire outside testers to probe their own defenses deliberately. These arrangements require contracts defining exactly what access is permitted. Any ambiguity in scope can trigger unintended criminal exposure. Testers who step slightly beyond agreed boundaries risk facing full prosecution. Current law offers no specific carve-out for these authorized testing arrangements. Prosecutors must interpret ordinary consent principles within a rigid framework. This creates uncertainty for companies designing lawful bug bounty programs today. Some firms hesitate to run these programs given unclear legal risk. Recent scholarship calls for tailored rules governing authorized penetration testing activities. Such rules would clarify boundaries between lawful testing and criminal intrusion. Without reform, valuable proactive security work remains legally uncertain in Italy. This gap slows adoption of modern, testing-based cyber security practices generally. Closing it would encourage safer, more transparent corporate security practices (Ruskevich, 2026).

Cross-border enforcement presents a further major challenge for Italian authorities. Cyber attacks routinely originate from servers located far outside national territory. Italian police need cooperation from foreign governments to gather key evidence. Different countries apply different legal standards for cybercrime investigation and evidence. This inconsistency slows down cases that involve multiple overlapping jurisdictions. Extradition and mutual legal assistance procedures often take considerable time to complete. Meanwhile, attackers can quickly move data, funds, and infrastructure elsewhere. Global cyber security regulation remains fragmented across many different legal systems worldwide. Some regions lack robust cybercrime laws entirely, creating convenient safe havens. This fragmentation directly weakens enforcement of Article 615-ter in practice. International initiatives increasingly push for greater regulatory harmonization across borders. Shared frameworks could streamline evidence sharing and joint investigation

efforts significantly. Until such harmonization improves, Italian prosecutors face real practical limits. Strong domestic law alone cannot fully solve inherently global cybercrime problems (AllahRakha, 2024).

Italy's broader digital transition also strains how courts apply older statutes. Article 615-ter was written before today's cloud systems and mobile networks existed. New technology often does not fit cleanly into older legal categories. Judges must stretch existing definitions to cover unfamiliar situations. This stretching risks inconsistent rulings across different Italian courts. Law enforcement agencies also need updated skills for digital investigation work. Officers trained years ago may struggle with newer forms of intrusion. Ongoing digital transformation is reshaping what effective law enforcement now requires. Some scholars describe this shift as a new face for policing. Training programs and specialized cybercrime units try to close this widening gap. Still, resource limits slow how quickly agencies can fully modernize. Smaller police departments often lack dedicated cybercrime expertise or equipment. This uneven capacity creates inconsistent enforcement across Italian regions today. Bridging this gap remains essential for applying Article 615-ter effectively (Morgante, 2025).

Evidence gathering itself creates real challenges when applying Article 615-ter. Investigators often need automated tools to gather data from online sources. Techniques like automated web scraping raise their own separate legal and ethical questions. Collecting evidence this way can accidentally sweep in personal information. This risks conflicting with data protection rules while building a case. Investigators must balance thorough evidence collection against strict privacy safeguards. Courts then face hard questions about admissibility of automatically gathered evidence. Some evidence may be challenged simply because collection methods remain legally unclear. This uncertainty can weaken otherwise strong prosecutions. Clearer guidelines on lawful digital evidence collection remain genuinely needed today. Without them, prosecutors risk losing cases over procedural disputes. Technology keeps advancing faster than rules governing digital evidence gathering. This constant gap complicates the consistent, reliable application of existing criminal provisions. Modern investigations therefore require careful attention to both law and technique (Kazmali, 2025).

Resource and training limits form a final major challenge for enforcement. Specialized cybercrime units remain small compared to digital crime. Many police stations still lack staff trained in advanced digital forensics. This shortage slows investigation timelines and delays court proceedings. Judges and defense lawyers also need stronger technical understanding of these cases. Without that understanding, courtroom arguments can become confused or oversimplified. Budget constraints further limit investment in modern investigative software and hardware. Smaller agencies often cannot afford the same tools as larger units. This creates uneven enforcement quality across different parts of Italy. Coordination between local police, national agencies, and courts needs improvement. Better information sharing could speed up investigations and reduce duplicated effort. Ongoing national cyber security initiatives aim to strengthen training and shared resources. These efforts remain a work in progress rather than a finished solution. Closing this resource gap is essential for consistently applying Article 615-ter (Allah Rakha, 2024).

Lawmakers should draft the amendment with clear, narrow legal language throughout. Vague wording invites inconsistent court rulings and confused enforcement. Every key term needs a precise definition within the text. Terms like intrusion, defensive action, and proportionate response need careful boundaries. Drafters should study existing debates between current law and proposed future reform. Legal scholars already discuss how Italian cybercrime law should evolve going forward. Their analysis offers a useful base for shaping precise amendment language. Lawmakers should also consult prosecutors and defense lawyers during the drafting process. Practical courtroom experience often reveals gaps theory alone cannot predict. Public consultation would strengthen legitimacy before final parliamentary approval. Clear language reduces future litigation over ambiguous or contested legal terms. It also helps companies understand what conduct remains lawful. Precise drafting forms the essential first step toward effective implementation. Getting this foundation right will shape every later stage of reform (Pepoli, 2022).

Implementation requires a legal principle giving this exception direct effect. Courts need clear authority to apply the amendment without extra steps. Legal systems can struggle when new rules lack immediate force. A direct-effect approach would let judges apply the exception right away. This avoids years of confusing transitional case law before settling. European legal theory already offers useful models for such implementation. Lawmakers can adapt these principles to fit the Italian legal system. Clear guidance should accompany the amendment from its first day. Ministry of Justice guidelines could help judges apply the provision consistently. Training materials should explain how courts should assess each defensive case. This reduces the risk of different outcomes across separate courtrooms. Consistent early application builds public and corporate trust in the rule. Without guidance, early rulings could create confusing or contradictory precedents. Careful implementation planning matters just as much as good drafting (Gruodytė et al., 2020).

Regulators should build differentiated response rules for different threat levels. Not every intrusion deserves the same defensive response. Minor probing attempts differ greatly from serious, coordinated criminal operations. Research on organized crime already shows how varied criminal activity is. That variety suggests cyber threats deserve a tiered legal approach. Simple defensive logging might suit minor incidents without triggering full countermeasures. More serious, sustained attacks could justify stronger, closely supervised defensive action. Regulators should publish clear examples illustrating each threat tier in real practice. This helps companies judge which response level fits their specific situation. Prosecutors would also benefit from consistent tiered guidance during case review. Such guidance reduces arbitrary decisions about when countermeasures become justified. It also discourages companies from overreacting to relatively minor incidents. A tiered system reflects real differences within the broader cybercrime landscape. This nuanced approach improves both fairness and practical implementation overall (Lavorgna & Sergi, 2014).

Implementation should include specific rules for high-risk critical sectors. Healthcare, energy, and financial systems face uniquely dangerous cyber attack risks. Attacks on medical devices can directly threaten patient safety. Recent research already documents serious vulnerabilities across many medical device systems. This growing risk shows why sector-specific defensive rules deserve special legal attention. A single general standard may not fit every industry's risk profile. Regulators should work closely with sector specialists when drafting these rules. Healthcare providers understand technical risks that generalist lawmakers may miss. Energy and finance sectors similarly need input from their own technical experts. This collaborative approach produces realistic and enforceable defensive standards. Sector-specific rules also help align the amendment with existing safety regulations. Overlapping rules without coordination could create confusing or contradictory compliance duties. Careful sector-based tailoring therefore strengthens both safety and legal clarity. This targeted approach makes implementation more practical across different industries (Bracciale et al., 2023).

Successful implementation also depends on proper judicial and police training. Judges need practical education on technical concepts behind cyber intrusions. Understanding attribution, proportionality, and necessity needs more than legal theory. Specialized courses could combine legal principles with real technical examples. Police investigators similarly need updated skills for handling digital evidence. Modern forensic tools require regular training to keep pace with technology. National judicial schools should build dedicated modules covering this specific amendment. Prosecutors should receive practical case studies showing how courts might apply it. Regular workshops could keep legal professionals updated as case law develops. This ongoing education prevents knowledge from becoming outdated within a few years. Well-trained judges apply new rules more consistently across different courtrooms. Consistent application builds public confidence in the amended legal framework. Without proper training, even well-written law risks uneven or unfair application. Investment in people therefore matters as much as investment in legal text.

Italy should pursue closer international cooperation alongside this domestic reform. Cyber attacks rarely stay confined within a single national border. Fast, reliable evidence sharing with foreign authorities remains genuinely essential. Italy should strengthen existing treaties governing digital evidence and extradition procedures. Faster response times would help preserve evidence before attackers can hide it. Joint investigation teams could handle complex cases spanning multiple countries efficiently. The European Union already promotes greater cooperation through several ongoing initiatives. Italy should actively participate in these regional cyber security cooperation efforts. Shared threat intelligence platforms could help Italian authorities detect emerging attack patterns. Regular coordination meetings with neighboring countries could strengthen practical cooperation further. Italy might also support harmonized cybercrime definitions across European Union member states. Consistent definitions make cross-border prosecution and cooperation considerably easier. Without strong international ties, domestic reform alone offers only partial protection. Global cooperation therefore complements rather than replaces careful domestic legal reform.

Italy should implement this amendment gradually, through a carefully phased approach. A pilot period could test the rule within a limited number of cases. Regulators could then review early outcomes before a broader rollout. This phased method allows quick correction of unexpected practical problems. Rushing full implementation risks locking in flawed procedures nationwide. Regular monitoring should track how courts and companies use the exception. Independent researchers could evaluate whether the amendment achieves its intended purpose. Annual reports could summarize case outcomes and emerging enforcement patterns. Lawmakers should remain open to revising the amendment based on evidence. Cyber security threats keep changing, so legal tools must stay similarly adaptable. Building review mechanisms directly into the law supports this ongoing flexibility. Stakeholders, including companies and civil society, should have input during reviews. This inclusive, evidence-based approach improves

legitimacy and practical effectiveness. Thoughtful, phased implementation gives this important reform its best chance of success.

Lawmakers should draft the amendment with clear, narrow legal language throughout. Vague wording invites inconsistent court rulings and confused enforcement. Every key term needs a precise definition within the text. Terms like intrusion, defensive action, and proportionate response need careful boundaries. Drafters should study existing debates between current law and proposed future reform. Legal scholars already discuss how Italian cybercrime law should evolve going forward. Their analysis offers a useful base for shaping precise amendment language. Lawmakers should also consult prosecutors and defense lawyers during the drafting process. Practical courtroom experience often reveals gaps theory alone cannot predict. Public consultation would strengthen legitimacy before final parliamentary approval. Clear language reduces future litigation over ambiguous or contested legal terms. It also helps companies understand what conduct remains lawful. Precise drafting forms the essential first step toward effective implementation. Getting this foundation right will shape every later stage of reform (Pepoli, 2022).

Implementation requires a legal principle giving this exception direct effect. Courts need clear authority to apply the amendment without extra steps. Legal systems can struggle when new rules lack immediate force. A direct-effect approach would let judges apply the exception right away. This avoids years of confusing transitional case law before settling. European legal theory already offers useful models for such implementation. Lawmakers can adapt these principles to fit the Italian legal system. Clear guidance should accompany the amendment from its first day. Ministry of Justice guidelines could help judges apply the provision consistently. Training materials should explain how courts should assess each defensive case. This reduces the risk of different outcomes across separate courtrooms. Consistent early application builds public and corporate trust in the rule. Without guidance, early rulings could create confusing or contradictory precedents. Careful implementation planning matters just as much as good drafting (Gruodytė et al., 2020).

Regulators should build differentiated response rules for different threat levels. Not every intrusion deserves the same defensive response. Minor probing attempts differ greatly from serious, coordinated criminal operations. Research on organized crime already shows how varied criminal activity is. That variety suggests cyber threats deserve a tiered legal approach. Simple defensive logging might suit minor incidents without triggering full countermeasures. More serious, sustained attacks could justify stronger, closely supervised defensive action. Regulators should publish clear examples illustrating each threat tier in real practice. This helps companies judge which response level fits their specific situation. Prosecutors would also benefit from consistent tiered guidance during case review. Such guidance reduces arbitrary decisions about when countermeasures become justified. It also discourages companies from overreacting to relatively minor incidents. A tiered system reflects real differences within the broader cybercrime landscape. This nuanced approach improves both fairness and practical implementation overall (Lavorgna & Sergi, 2014).

Implementation should include specific rules for high-risk critical sectors. Healthcare, energy, and financial systems face uniquely dangerous cyber attack risks. Attacks on medical devices can directly threaten patient safety. Recent research already documents serious vulnerabilities across many medical device systems. This growing risk shows why sector-specific defensive rules deserve special legal attention. A single general standard may not fit every industry's risk profile. Regulators should work closely with sector specialists when drafting these rules. Healthcare providers understand technical risks that generalist lawmakers may miss. Energy and finance sectors similarly need input from their own technical experts. This collaborative approach produces realistic and enforceable defensive standards. Sector-specific rules also help align the amendment with existing safety regulations. Overlapping rules without coordination could create confusing or contradictory compliance duties. Careful sector-based tailoring therefore strengthens both safety and legal clarity. This targeted approach makes implementation more practical across different industries (Bracciale et al., 2023).

Successful implementation also depends on proper judicial and police training. Judges need practical education on the technical concepts behind intrusions. Understanding attribution, proportionality, and necessity needs more than legal theory. Specialized courses could combine legal principles with real technical examples. Police investigators similarly need updated skills for handling digital evidence. Modern forensic tools require regular training to keep pace with technology. National judicial schools should build dedicated modules covering this specific amendment. Prosecutors should receive practical case studies showing how courts might apply it. Regular workshops could keep legal professionals updated as case law develops. This ongoing education prevents knowledge from becoming outdated quickly. Well-trained judges apply new rules more consistently across courtrooms. Consistent application builds public confidence in the amended legal framework. Without proper training, even well-written law

risks uneven or unfair application. Investment in people therefore matters as much as investment in legal text (Jitariuc & Greco, 2020).

Italy should pursue closer international cooperation alongside domestic reform. Cyber attacks rarely stay confined within a single national border. Fast, reliable evidence sharing with foreign authorities remains essential. Italy should strengthen existing treaties governing digital evidence and extradition procedures. Faster response times would help preserve evidence before attackers can hide it. Joint investigation teams could handle complex cases spanning multiple countries efficiently. The European Union already promotes greater cooperation through several ongoing initiatives. Italy should actively participate in these regional cyber security cooperation efforts. Shared threat intelligence platforms could help Italian authorities detect emerging attack patterns. Regular coordination meetings with neighboring countries could strengthen practical cooperation further. Italy might also support harmonized cybercrime definitions across European Union member states. Consistent definitions make cross-border prosecution and cooperation considerably easier. Without strong international ties, domestic reform alone offers only partial protection. Global cooperation therefore complements rather than replaces careful domestic legal reform (Crescioli, 2024).

Italy should implement this amendment through a carefully phased approach. A pilot period could test the rule within a limited set of cases. Regulators could then review early outcomes before any broader rollout. This phased method allows quick correction of unexpected practical problems. Rushing implementation risks locking in flawed procedures nationwide. Regular monitoring should track how courts and companies use the exception. Independent researchers could evaluate whether the amendment achieves its intended purpose. Annual reports could summarize case outcomes and emerging enforcement patterns. Lawmakers should remain open to revising the amendment based on evidence. Cyber security threats keep changing, so legal tools must stay similarly adaptable. Building review mechanisms directly into the law supports this ongoing flexibility. Stakeholders, including companies and civil society, should have input during reviews. This inclusive, evidence-based approach improves legitimacy and practical effectiveness. Thoughtful, phased implementation gives this important reform its best chance of success (Matsuoka, 2020).

This research examined legal limits governing private active cyber defense. Current Italian law criminalizes nearly all corporate defensive action. This blanket approach no longer matches the realities of threats. Companies now possess real technical capability without matching legal permission today. The proposed amendment offers a narrow, carefully bounded solution to this gap. It grants limited defensive rights while preserving strong criminal protections. This balance reflects thoughtful engagement with security needs and legal caution. Broader European debates about innovation and regulation echo this same tension. Lawmakers everywhere struggle to update old rules without abandoning protections. Regulatory experimentation spaces already offer useful models for testing legal reform. Italy could similarly test this amendment before any permanent, nationwide change. Such caution reduces risk while still allowing meaningful progress. This research therefore contributes a concrete proposal within an ongoing European conversation. The path forward requires patience, careful drafting, and continuous legal review (Cirone, 2025).

The proposed reform also fits within a wider strategic view of cyber security. Effective cyber security requires more than reactive, incident-based legal responses. It needs coordinated planning across technology, policy, and legal institutions. Recent scholarship stresses this kind of integrated, strategic approach to defense. Legal reform works best when paired with technical and organizational preparedness. The amendment alone cannot solve every corporate cyber security challenge. It represents one piece within a much larger strategic puzzle. Companies still need strong internal security practices regardless of new permissions. Good governance, staff training, and updated technology remain essential elements. Legal defense tools should support, not replace, sound security management. This research situates its recommendations within that broader strategic context. Narrow legal reform gains real value only alongside sound organizational practice. Together, these elements create a more resilient cyber security posture. Future policy work should keep this connection between law and strategy in mind (AlDaajeh & Alrabae, 2024).

This study also highlights the human side behind cyber intrusions. Not every attacker fits a single, predictable criminal profile. Some individuals drift into cybercrime gradually, while others plan it. Criminological research on organized crime shows similarly varied entry routes. People join or found criminal enterprises for different personal reasons. This diversity matters when designing fair, proportionate legal responses. A rigid, one-size-fits-all framework risks ignoring these important differences. The proposed amendment's focus on intent partly reflects this deeper insight. Recognizing varied motives supports more nuanced prosecutorial and judicial decision-making. It also reminds policymakers that deterrence alone cannot solve everything. Broader social and economic factors often shape pathways into cybercrime too. Addressing only the technical and legal sides misses part of the picture. Future research

should continue exploring these human dimensions of cyber offending. Understanding offenders, not just their code, remains essential for lasting policy success (Kemp & Van der Hulst, 2020).

This research also touches on the growing role of digital intermediaries. Platforms and network operators often sit between attackers and their victims. Legal scholarship increasingly examines what responsibility these intermediaries should bear. New categories of digital intermediary now trigger evolving forms of legal liability. This evolution matters directly for how the proposed amendment might operate. A defending company may need cooperation from intermediaries during an active intrusion. Clear rules about intermediary responsibility could support faster, more effective defensive action. Without such clarity, companies may face delays when seeking urgent technical assistance. Future legal reform should therefore consider intermediary duties alongside corporate defense rules. Coordinated obligations across different actors create a more coherent legal system. This connection deserves further attention beyond the scope of this particular study. Recognizing these links strengthens the case for comprehensive cyber security legal reform. Isolated fixes rarely address problems that span multiple actors and layers (Allegri, 2021).

European data and platform law keeps evolving alongside cyber security regulation. Recent summaries of this evolution show a clear pattern of change. New rules on data governance regularly interact with existing criminal provisions. This overlapping landscape adds complexity for lawmakers drafting the amendment. Any defensive exception must stay consistent with parallel data governance duties. Ignoring this wider context risks creating conflicting or duplicated legal requirements. Italian lawmakers should track these parallel developments during drafting. Coordination between regulatory bodies would help avoid contradictory compliance demands. This coordination becomes especially important as more digital laws take effect. A fragmented regulatory approach ultimately burdens companies trying to fully comply. Streamlined, coherent regulation benefits both enforcement authorities and businesses alike. This research recommends viewing the amendment within this evolving regulatory map. Future legal analysis should keep tracking how these frameworks interact. Only sustained, active attention can keep pace with such rapid regulatory change (Lobascio, 2024).

Finally, this research fits within a wider global conversation on cyber law. Countries beyond Italy also work to update older cybercrime statutes. Recent studies examine how nations like Uzbekistan safeguard digital spaces domestically. These efforts show shared global recognition of similar legal challenges. Different legal traditions still produce varied solutions to similar problems. Studying these varied approaches offers useful lessons for future reform. No single country has yet found a perfect legal model. Continuous learning across jurisdictions stays valuable given how fast threats evolve. Italy's proposed amendment adds one thoughtful contribution to this global legal effort. It reflects careful balancing between corporate needs and public accountability. Future research could examine how similar amendments perform in practice. Tracking real-world outcomes would help refine this and similar reforms. This research closes not with full certainty, but with a clear path forward. Continued dialogue between scholars, lawmakers, and practitioners remains essential (AllahRakha, 2023).

CONCLUSION

Private companies now stand at a legal crossroads when cyber attacks strike. They possess growing technical power but lack matching legal permission. This research asked what legal limits should shape private active cyber defense. The question matters because attacks keep rising while legal clarity lags behind. Companies caught between real threats and rigid criminal law face genuine danger. A wrong move could trigger prosecution instead of protection for the defending firm. This tension sits within a much larger global struggle over digital governance. Nations everywhere debate how much power private actors should reasonably hold online. Italy's Article 615-ter offers one clear example of this widespread legal gap. Its strict wording reflects an era before modern, organized cyber attacks existed. Rethinking this statute speaks to challenges facing legal systems well beyond Italy. The stakes extend past any single company or single national jurisdiction. This research therefore addresses a problem with meaningful, wide-reaching consequences.

Three main findings emerged from this close legal examination of the topic. First, international law grants corporations no independent right to self-defense online. State-focused legal doctrine simply does not extend to private cyber responses. Second, Italian criminal law currently treats every unauthorized access as identical wrongdoing. It ignores intent, proportionality, and the realistic pressures companies face during attacks. Third, a carefully limited defensive exception could close this gap responsibly. Such an exception would require proof of active intrusion and genuine necessity. It would also demand strict proportionality and mandatory reporting to regulators.

These findings connect through one shared thread running across the entire analysis. Legal permission must expand carefully, never carelessly, alongside growing corporate capability. Reform without limits risks turning defense into unchecked private retaliation instead. Reform without any change leaves companies stuck between danger and criminal liability. Balancing these forces remains the central challenge running through this entire study.

These findings carry weight far beyond academic legal debate. Lawmakers across Europe face similar pressure to modernize old cybercrime statutes. Companies in finance, healthcare, and energy face this exact uncertainty today. A clearer legal standard would let these firms respond faster during real attacks. It would also protect innocent parties from careless corporate action. Regulators could apply this research's proposed conditions directly during future legislative drafting. Courts could use the same conditions when deciding early cases under new rules. Many questions still remain open for scholars and policymakers to explore further. Researchers should study how similar reforms perform once actually put into practice. Comparative studies across different countries could reveal which safeguards work best. Attention should also turn toward protecting ethical hackers who test system security. Ongoing digital transition will keep testing whether legal systems can adapt quickly. This research offers one careful step toward answering that pressing modern question.

BIBLIOGRAPHY

- Akande, D., & Liefländer, T. (2013). Clarifying necessity, imminence, and proportionality in the law of self-defence. *American Journal of International Law*, 107(3), 563–572. <https://doi.org/10.5305/amerjintlaw.107.3.0563>
- AlDaa'jeh, S., & Alrabaa, S. (2024). Strategic cybersecurity. *Computers & Security*, 141, 103845. <https://doi.org/10.1016/j.cose.2024.103845>
- AllahRakha, N. (2023). Cyber law: Safeguarding digital spaces in Uzbekistan. *International Journal of Cyber Law*, 1(5). <https://doi.org/10.59022/ijcl.53>
- AllahRakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2), 23–54. <https://doi.org/10.22201/ij.24485306e.2024.2.18892>
- AllahRakha, N. (2024). Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. *Lex Scientia Law Review*, 8(1), 405–432. <https://doi.org/10.15294/lslr.v8i1.2081>
- Allegri, M. R. (2021). Le categorie di intermediari digitali e le nuove forme di responsabilità. *Rivista Italiana di Informatica e Diritto*, 3(2), 7–23. <https://doi.org/10.32091/RIID0036>
- Barnes, I. A. (2018). Implementation of active cyber defense measures by private entities: The need for an international accord to address disputes. *Homeland Security Affairs*. <https://www.hsaj.org/articles/14933>
- Bracciale, L., et al. (2023). Cybersecurity vulnerability analysis of medical devices. *Scientific Reports*, 13, 18592. <https://doi.org/10.1038/s41598-023-45927-1>
- Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, 7(1), tyab010. <https://doi.org/10.1093/cybsec/tyab010>
- Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, 53, 105961. <https://doi.org/10.1016/j.clsr.2024.105961>
- Cirone, E. (2025). Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative. *Rivista Italiana di Informatica e Diritto*, 7(1), 257–278. <https://doi.org/10.32091/RIID0211>
- Cook, C. (2018). Cross-border data access and active cyber defense: Assessing legislative options for a new international cybersecurity rulebook. *Stanford Law & Policy Review*, 29(2), 235–268.

- Crescioli, C. (2024). La lucha contra el cibercrimen y las últimas reformas penales en España e Italia: luces y sombras. *Revista de Estudios Jurídicos y Criminológicos*, (10), 403–427. <https://doi.org/10.25267/REJUCRIM.2024.i10.12>
- Darem, A. A., Alhashmi, A. A., Alkhalidi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, 11, 125138–125158. <https://doi.org/10.1109/ACCESS.2023.3327016>
- Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers & Security*, 40, 108–113. <https://doi.org/10.1016/j.cose.2013.11.004>
- Dziwisz, D. (2024). Legalising forms of active cyber defense (ACD): The theory and practice of private cybersecurity provisioning. *Politeja*, 21(6), 135–160. <https://doi.org/10.12797/Politeja.21.2024.93.06>
- Fiorinelli, G. (2024). Il ransomware nel DDL Cybersicurezza: dalla fattispecie di estorsione "informatica" al coordinamento tra indagini e incident response. *Rivista Italiana di Informatica e Diritto*, 6(1), 35–39. <https://doi.org/10.32091/RIID0143>
- Flor, R. (2025). Cybersecurity e diritto penale. Verso la tutela di un bene giuridico di nuova generazione, tra passato, presente e prospettive future. *Ius Online*, 1, 106–127. <https://doi.org/10.3280/ius2025oa21816>
- Flor, R., & Panattoni, B. (2023). Digital criminal investigations in Italy: The intersection between data protection and cybersecurity. *New Journal of European Criminal Law*, 14(4), 456–475. <https://doi.org/10.1177/20322844231212836>
- Fusco, L. E. (2020). Los delitos informáticos en el Código Penal Italiano. *Derecho Global. Estudios sobre Derecho y Justicia*, 5(14), 127–149. <https://doi.org/10.32870/dgedj.v5i14.2505>
- Gerke, K. (2021). Canadian hack-back?: A consideration of the Canadian legal framework for private-sector active cyber defence. *Alberta Law Review*, 59(1), 171–200. <https://doi.org/10.29173/alr2668>
- Gruodytė, E., Milčiuvienė, S., & Palionienė, N. (2020). The principle of direct effect in criminal law: Theory and practice. *European Studies*, 7(1), 66–87. <https://doi.org/10.2478/eustu-2022-0047>
- Jasmontaite, L., Kamara, I., & Zanfiri-Fortuna, G. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, 4(2), 168–189. <https://doi.org/10.21552/edpl/2018/2/7>
- Jitariuc, V., & Greco, F. (2020). Investigative techniques in the digital age: Cybercrime and criminal profiling. *International Journal of Cyber Criminology*. <https://doi.org/10.5281/zenodo.3877668>
- Kazmali, A. S. (2025). Web scraping: Legal and ethical considerations in general and local context. *Procedia Computer Science*, 259, 1563–1572. <https://doi.org/10.1016/j.procs.2025.04.111>
- Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, 7(1), tyab014. <https://doi.org/10.1093/cybsec/tyab01>
- Kemp, L., & Van der Hulst, M. (2020). Pathways into organized crime: Comparing founders and joiners. *Trends in Organized Crime*, 23(3), 203–226. <https://doi.org/10.1007/s12117-019-09371-w>
- Kulesza, M. (2021). Criminalizing cybercrimes: Italian and Polish experiences. *Białostockie Studia Prawnicze*, 26(3), 115–130. <https://doi.org/10.15290/bsp.2021.26.03.09>
- Lavorgna, A., & Sergi, A. (2014). Types of organised crime in Italy: The multifaceted spectrum of Italian criminal associations. *International Journal of Law, Crime and Justice*, 42(1), 54–72. <https://doi.org/10.1016/j.ijlcrj.2013.11.002>
- Leventopoulos, S., Pipiros, K., & Gritzalis, D. (2024). Retaliating against cyber-attacks: A decision-taking framework for policy-makers and enforcers of international and cybersecurity law. *International Cybersecurity Law Review*, 5, 237–262. <https://doi.org/10.1365/s43439-024-00113-5>

- Lobascio, C. (2024). Tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme. *Rivista Italiana di Informatica e Diritto*. <https://doi.org/10.32091/RIID0173>
- Matsuoka, A. (2020). Remember the balance of forces. *Journal of Financial Crime*, 27(4), 1379–1388. <https://doi.org/10.1108/JFC-09-2019-0119>
- Meccariello, T. (2026). Il cyberspazio tra impostazioni tradizionali e consolidamento normativo della 'riservatezza'. *Rivista Italiana di Informatica e Diritto*, 7(2), 139–146. <https://doi.org/10.32091/RIID0257>
- Morgante, G. (2025). Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del law enforcement. *Rivista Italiana di Informatica e Diritto*, 7(2). <https://doi.org/10.32091/RIID0254>
- Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, 5(2), 233–254. <https://doi.org/10.1017/eis.2020.6>
- Pepoli, V. S. Z. B. (2022). Profili di contrasto al cybercrime in iure condito e de iure condendo. *Rivista Italiana di Informatica e Diritto*, 4(2), 109–121. <https://doi.org/10.32091/RIID0087>
- Perri, P., & Zanero, S. (2004). Lessons learned from the Italian law on privacy – Part II. *Computer Law & Security Report*, 20(5), 354–360. [https://doi.org/10.1016/S0267-3649\(04\)00069-X](https://doi.org/10.1016/S0267-3649(04)00069-X)
- Pietropaoli, S. (2024). Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza. *Rivista Italiana di Informatica e Diritto*, 1(1), 106–127. <https://doi.org/10.32091/RIID0153>
- Rampášek, M., Andraško, J., Sokol, P., & Hamulak, O. (2026). Hunting for vulnerabilities: Call for European protection of ethical hackers. *Journal of Cybersecurity*, 12(1). <https://doi.org/10.1093/cybsec/tyag002>
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Russkevich, E. A. (2026). Criminal law compliance with cyber resilience testing of information systems: Penetration testing and bug bounty. *Legal Issues in the Digital Age*, 7(1), 141–163. <https://doi.org/10.17323/2713-2749.2026.1.141.163>
- Sánchez-García, I. D., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Computers & Security*, 128, 103170. <https://doi.org/10.1016/j.cose.2023.103170>
- Thumfart, J. (2020). Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius. *Internet Policy Review*, 9(3). <https://doi.org/10.14763/2020.3.1500>
- Zlati, G. (2024). Romanian jurisprudence on cybercrime: Focus on illegal access to an information system. *ERA Forum*, 25(3), 425–440. <https://doi.org/10.1007/s12027-024-00810-y>