sciendo

Protecting dual-use technological innovation through trade secret law: institutional limits and cybersecurity challenges

Lisette Põld

School of Law
University of Tartu
Tõnismägi 5a
Tallinn 10119, Estonia
lisette.pold@ut.ee

Abstract: This article examines the institutional limits of EU trade secret law in the context of contemporary cyberthreats targeting dual-use technological innovation. It also explores the extent to which the EU Trade Secrets Directive ('Council directive 2016/943') can effectively protect strategically sensitive technological information against systemic, automated, and difficult-to-attribute cyber operations, and identify where complementary governance tools are required. Using doctrinal, comparative, and functional analyses informed by existing empirical studies, the study examines legal developments in this area in Estonia, Germany, and France. It demonstrates that effective protection of strategically sensitive innovation increasingly depends less on *ex post* legal remedies and more on organisational resilience, cybersecurity governance, and preventive risk management. The article further evaluates the relationship between trade secrets and selective patent disclosure within broader innovation-security strategies, arguing that trade secrets must be embedded in a layered protection model rather than treated as a self-sufficient mechanism.

Keywords: *cybersecurity, intellectual property law, patent law, technological innovation, trade secrets*

https://doi.org/10.2478/bjes-2026-0028 *TalTech Journal of European Studies*, 16(2(45))
Tallinn University of Technology (ISSN 2674-4619)

1. Introduction

Technological innovation increasingly constitutes not only an economic asset but also a strategic resource within contemporary geopolitical competition. In highly digitalised knowledge economies, control over intangible technological information shapes both economic power and strategic autonomy (van Dijk, 2017, p. 6; Duguin and Pavlova, 2023, p. 14). At the same time, the growing prevalence of cyber espionage, automated data extraction, and state-sponsored cyber operations challenges the underlying assumptions of traditional intellectual property (hereafter IP) protection mechanisms, particularly where technological innovation possesses dual-use potential. Figuratively speaking, the same microchip may power both a consumer device and a weapons system (Rutiku, 2025).

Trade secrets are particularly significant in sectors where innovation is increasingly protected through confidentiality, contractual control, software development, and know-how, rather than through patents. Unlike classical intellectual property rights (hereafter IPRs), trade secret protection does not confer an exclusive right granted by the state but instead depends on the continued maintenance of secrecy and the ability to prevent unlawful acquisition, use, or disclosure. Although trade secrets are frequently associated with the broader field of IP law, their legal nature remains conceptually ambiguous. As has been noted in legal scholarship, "[n]o international consensus has developed regarding the classification of trade secrets; is it or is it not an Intellectual Property Right?", while it has further been observed that 'Council directive (EU) 2016/943' (2016) (hereafter Trade Secrets Directive) itself does not formally regard trade secrets as IPRs (Riis and Schovsbo, 2019, p. 1). Nevertheless, trade secrets increasingly perform functions comparable to those of IPRs in innovation-driven economies and have become an important component of the European Union (hereafter EU) innovation protection framework under the Trade Secrets Directive. Consequently, trade secret protection is especially vulnerable in cyber environments characterised by anonymity, automation, and difficulties in attribution.

This creates a structural tension within EU trade secret law. The enforcement architecture established by the Trade Secrets Directive is largely premised on identifiable acts of unlawful acquisition or disclosure by attributable actors. However, contemporary cyberthreats increasingly operate through systemic, automated, or state-linked activities that often remain undetected or legally

non-attributable. As a result, the effectiveness of trade secret protection increasingly depends not only on legal remedies but also on organisational resilience, cybersecurity governance, and preventive risk management.

This article examines the institutional limits of EU trade secret law in the context of contemporary cyberthreats affecting dual-use technological innovation. It argues that although the Trade Secrets Directive establishes a harmonised legal framework for protecting confidential business information, its predominantly *ex post* and actor-based enforcement model encounters significant limitations in cyber environments characterised by automation, cross-border operations, and difficulties in attribution. More broadly, trade secret protection cannot be understood solely as an isolated IP mechanism but must instead be situated within a broader framework encompassing cybersecurity regulation, organisational governance, and strategic technological resilience. Within this framework, selective patent disclosure is analysed not as a competing paradigm but as a complementary mechanism for managing the exposure of dual-use technological information where secrecy alone is insufficient.

The study focuses on Estonia, Germany, and France because these jurisdictions represent distinct approaches to the integration and application of the Trade Secrets Directive within the EU. Germany and France represent two of the most influential civil-law traditions in the EU following the United Kingdom's withdrawal. At the same time, Estonia provides a particularly relevant case study as a highly digitalised economy whose innovation ecosystem relies comparatively more on software, IT services, copyright, and trade secrecy than on patent-intensive industrial innovation. In addition, Estonian private law has historically developed under significant German doctrinal influence, making the comparison methodologically instructive. Together, these jurisdictions illustrate how formally harmonised trade secret rules continue to produce different enforcement cultures, evidentiary expectations, and approaches to technological risk.

Methodologically, the article combines doctrinal legal analysis with comparative and functional approaches. It examines legislation, case law, and legal scholarship on trade secret protection, drawing selectively on empirical reports and case-law collections that illuminate litigation patterns, while also analysing how contemporary cyberthreats challenge the institutional assumptions underlying existing IP frameworks. Section 1 revisits the concept of trade secrets in EU and national law (Estonia, Germany, and France). Section 2 assesses the effectiveness and practical

limits of judicial enforcement in contemporary cyber contexts. Section 3 examines the reasonable-steps requirement and its interaction with cybersecurity governance. Section 4 analyses reverse engineering and the role of selective patent disclosure within a layered protection strategy. The article's original contribution lies in connecting these doctrinal elements to concrete cyberthreat scenarios and demonstrating that EU trade secret law can function effectively only as one component of a broader innovation-security framework.

The article also evaluates the relationship between trade secrets and selective patent disclosure, assessing their respective roles in protecting dual-use technological innovation in a changing geopolitical environment. It concludes that even though trade secret law remains a flexible and commercially important protection mechanism, its practical effectiveness increasingly depends on complementary cybersecurity governance and broader innovation-security strategies rather than private-law enforcement alone.[1]

2. Revisiting the definition of trade secrets in contemporary EU law and cyber contexts

The Trade Secrets Directive harmonises key aspects of trade secret protection within the EU, including the definition of a trade secret, the distinction between lawful and unlawful acquisition, and a minimum framework of civil remedies, while leaving procedural matters largely to national law. This section first outlines the core definition of the concept and then highlights those elements that become particularly salient in cyber environments.

According to Article 2(1) of the Trade Secrets Directive, a trade secret is information that is not generally known or readily accessible, possesses commercial value because of its secrecy, and is subject to reasonable steps intended to preserve confidentiality. These cumulative criteria form the conceptual foundation of EU trade secret protection and become particularly significant in contemporary cyber environments characterised by automated data extraction, cyber espionage, and difficulties in attribution.

[1] The author used generative AI tools, including OpenAI's ChatGPT, Perplexity, and Grammarly, to improve linguistic clarity, structure, and reference verification. All substantive arguments, legal analysis, and conclusions are the result of the author's independent research and reasoning.

Although the Trade Secrets Directive does not formally classify trade secrets as IPRs, trade secrets increasingly fulfil functions comparable to those performed by conventional forms of IP protection in innovation-driven economies (Riis and Schovsbo, 2019, p. 1). Technological trade secrets commonly include manufacturing processes, technical know-how, software-related innovation, prototypes, designs, and production methods (Varadarajan, 2014, p. 30). In practice, disputes frequently concern manufacturing processes and technical know-how, followed by prototypes and unreleased product designs (EUIPO, 2023, p. 30). As technological innovation increasingly acquires strategic and dual-use significance, trade secret protection also intersects with broader questions of cybersecurity governance and technological resilience.

Although Estonia, Germany, and France now operate within the harmonised framework established by the Trade Secrets Directive, these jurisdictions were selected because they represent different approaches to the application and implementation of trade secret protection within the EU. Germany and France have comparatively well-developed and influential legal frameworks governing trade secrets. At the same time, Estonia offers a relevant example of a highly digitalised economy whose innovation ecosystem relies comparatively more on software, IT services, and trade secrecy. Together, these jurisdictions illustrate how formally harmonised rules continue to produce different judicial and evidentiary approaches in contemporary cyber contexts. Before the implementation of the Trade Secrets Directive, all three jurisdictions protected confidential, valuable business information through combinations of unfair competition law, tort law, contractual obligations, and employment-related confidentiality duties. However, the structure and doctrinal sophistication of these systems differed considerably.

Germany already possessed a comparatively developed framework centred on unfair competition and criminal law provisions under the *Act against Unfair Competition (Germany) 2004* (*Gesetz gegen den unlauteren Wettbewerb*, hereafter UWG), supplemented by civil-law remedies under the *Civil Code (Germany) 1896* (*Bürgerliches Gesetzbuch*, hereafter BGB) (Hoeren, 2018, p. 138; Ohly, 2020, p. 1). The implementation of the Trade Secrets Directive through the *Law on the Protection of Trade Secrets (Germany) 2019* (*Gesetz zum Schutz von Geschäftsgeheimnissen*, hereafter GeschGehG) primarily reorganised and clarified existing principles within a coherent civil-law framework. German courts have since developed the most structured body of jurisprudence concerning the reasonable steps requirement, emphasising proportionality, sector-specific practices, organisational controls, and

evidentiary precision (Munich Regional Court, 2019, para. 25; Stuttgart Higher Regional Court, 2020, paras. 277–278, 381, 386; Federal Labour Court, 2024, para. 37). The German approach, therefore, reflects a comparatively systematic and doctrine-oriented understanding of trade secret protection.

France, by contrast, has historically relied on a fragmented combination of general tort law under the *Civil Code (France) 1804* (*Code civil*), labour law duties of loyalty under the *Labour Code (France) 1910* (*Code du travail*), and sector-specific confidentiality provisions without recognising trade secrets as an autonomous legal category (Gougé and Truchot-Bothner, 2019, p. 187). The implementation of the Trade Secrets Directive through *Law No. 2018-670 (France) 2018*, now incorporated into the *Commercial Code (France) 1807* (*Code de commerce*), introduced a dedicated statutory framework for trade secret protection. Nevertheless, French courts continue to approach disputes predominantly through flexible and fact-specific reasoning rather than through highly formalised doctrinal analysis (Gougé and Truchot-Bothner, 2019, p. 141). The Court of Cassation (2025) has confirmed that trade secret protection must be assessed in accordance with the statutory criteria established by the Trade Secrets Directive, while balancing competing interests and exceptions.

Estonia represents a more recent transition from a fragmented confidentiality regime to harmonised statutory protection. Before the implementation of the Trade Secrets Directive, protection was derived largely from general private law under the *Law of Obligations Act (Estonia) 2001* (*Võlaõigusseadus*), unfair competition rules under the *Competition Act (Estonia) 2001* (*Konkurentsiseadus*), and contractual and employment-related confidentiality obligations under the *Employment Contracts Act (Estonia) 2008* (*Töölepinguseadus*) (Värv, 2020, p. 418; Värv *et al*., 2010, p. 333). This legacy explains why Estonian courts now apply the Trade Secrets Directive's criteria in a particularly formal and evidence-intensive manner, which has implications for cyber-related claims.

The implementation of the Trade Secrets Directive through the *Restriction of Unfair Competition and Protection of Business Secrets Act (Estonia) 2018* (*Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus*) introduced a unified statutory regime aligned with the Trade Secrets Directive's criteria. Estonian courts have subsequently adopted a comparatively strict and formal evidentiary approach, requiring precise identification of the protected information and demonstrable protective measures as prerequisites for protection (Supreme Court of Estonia, 2020a, paras. 40–41; 2020b, para. 6).

Judicial interpretation continues to rely partly on comparative foreign jurisprudence, particularly German legal doctrine (Supreme Court of Estonia, 2009, para. 10(2)).

Taken together, these jurisdictions demonstrate that harmonisation under the Trade Secrets Directive has not eliminated divergence in judicial reasoning, evidentiary expectations, or approaches to organisational secrecy measures. Germany reflects the most systematic jurisprudence on reasonable protective measures; France maintains a comparatively flexible, fact-based approach; and Estonia illustrates a more formalistic, evidence-intensive model with still limited jurisprudential development. These differences become particularly significant in contemporary cyber environments, where the practical effectiveness of trade secret protection increasingly depends not only on formal legal criteria but also on how legal systems address the challenges related to attribution, automated information extraction, and organisational cybersecurity governance.

3. Institutional limits of trade secret protection in contemporary cyber contexts

The comparative overview above demonstrates that, despite harmonisation under the Trade Secrets Directive, trade secret protection within the EU continues to depend heavily on evidentiary standards, organisational secrecy measures, and national enforcement practices. These structural characteristics become particularly significant in contemporary cyber environments, where technological innovation is increasingly exposed to automated, cross-border, and frequently non-attributable forms of information extraction.

Trade secret protection is fundamentally premised on several institutional assumptions: that confidential information can be identified with sufficient precision, that unlawful acquisition or disclosure can be detected, and that responsible actors can ultimately be identified and subjected to legal remedies. While these assumptions remain broadly workable in conventional forms of commercial misappropriation, they become increasingly difficult to sustain in digital environments characterised by cyber espionage, large-scale data extraction, and state-linked cyber operations targeting strategically valuable technological information.

The Trade Secrets Directive nevertheless provides a comprehensive framework of civil protection against unlawful acquisition, use, and disclosure. Under Article 4, read together with Chapter III, Member States must ensure the availability of remedies that are fair, effective, and dissuasive, including injunctive relief and damages. Judicial protection is available both before and after a finding of infringement. Articles 10 and 11 provide for provisional and final measures, including injunctions, cessation of use, and the withdrawal of infringing goods, while Articles 12 and 14 regulate compensation for economic loss, unjust enrichment, and hypothetical royalties.

3.1 Practical limits of judicial enforcement

Article 9 of the Trade Secrets Directive further introduces procedural safeguards intended to preserve confidentiality during litigation itself. These include restrictions on access to documents, confidentiality orders, and limitations on participation in hearings. National courts have recognised the importance of such measures in ensuring effective judicial protection. In Estonia, for example, the Supreme Court has held that trade secrets fall within the interests protected under Section 24(3) of the *Constitution of the Republic of Estonia 1992*, thereby permitting proceedings, or parts thereof, to be conducted in closed session for the protection of confidential information (Supreme Court of Estonia, 2008, para. 20).

Nevertheless, the practical implementation of confidentiality safeguards continues to vary considerably across Member States, and the Trade Secrets Directive has been criticised for providing only limited procedural guidance (Farkas and Koch, 2016; Schröder and Widera, 2021).

Despite this formally extensive enforcement architecture, trade secret litigation remains comparatively limited in practice. Empirical evidence indicates that proceedings frequently encounter significant evidentiary difficulties concerning the identification of the protected information, proof of secrecy, and demonstration of unlawful conduct (EUIPO, 2023, pp. 35, 345). Trade secrets often consist of complex and composite bodies of technical information that are difficult to define with precision. As a result, one of the most common defences raised in litigation is that the information at issue does not qualify as a trade secret because it is generally known or readily accessible (EUIPO, 2023, p. 35).

The economic realities of complex litigation reinforce these evidentiary challenges. Although no comprehensive data exist concerning the costs of

trade secret litigation in Europe, patent litigation provides a useful point of comparison because of its comparable technical and evidentiary complexity. Studies indicate that first-instance patent litigation costs in jurisdictions such as Germany, France, and the Netherlands may range from approximately 50,000 to 350,000 euros, with substantially higher costs in particularly complex disputes (Rantasaari, 2023, pp. 644–645). Such financial burdens may significantly discourage enforcement, particularly among small and medium-sized enterprises whose innovation strategies depend heavily on confidential know-how rather than formal IP registration.

At the same time, contemporary cyber environments expose the structural limits of *ex post* enforcement. Once confidential information has been extracted through cyber intrusion or unauthorised digital access, its subsequent dissemination may become practically impossible to trace or contain. This significantly weakens the restorative function of litigation, since secrecy, once irreversibly compromised, cannot easily be restored through judicial remedies alone (Bone, 2011, p. 4). The problem is further exacerbated by the fact that many contemporary cyber operations are specifically designed to avoid attribution. Unauthorised extraction of technological information may occur through automated processes, anonymised digital infrastructures, or state-linked cyber activities operating across multiple jurisdictions.

These developments expose a fundamental limitation within the institutional logic of trade secret protection. The Trade Secrets Directive remains largely structured around conventional models of commercial misappropriation involving identifiable actors, attributable conduct, and legally observable breaches of confidence. Contemporary cyberthreats frequently operate outside these assumptions. Even where unlawful acquisition may be strongly suspected, establishing causation, attribution, and the necessary evidentiary basis for a claim may remain legally or technically impossible.

Similar limitations can also be observed in criminal-law frameworks. National criminal provisions concerning unlawful disclosure of trade secrets and cyber intrusion continue to depend primarily on identifiable actors and attributable conduct. They are therefore considerably less effective against systemic, automated, or state-linked cyber espionage operations targeting commercially valuable technological innovation. This does not render the trade secret doctrine internally incoherent. Rather, these difficulties illustrate the institutional limits of private-law enforcement mechanisms when applied to cyber environments characterised by anonymity, automation, and strategic technological targeting.

3.2 From remedies to prevention

These structural constraints help explain why the practical centre of gravity of trade secret protection is increasingly shifting from *ex post* judicial remedies towards *ex ante* prevention. In practice, preventing disclosure is considerably more important than attempting to restore secrecy after compromise has already occurred. Once confidential information loses its secrecy, its commercial value may be impossible to recover fully, even through successful litigation (Schröder and Widera, 2021).

Within this context, the reasonable-steps requirement under Article 2(1)(c) of the Trade Secrets Directive assumes central importance. The requirement performs not only a doctrinal function in defining protected information, but also a broader governance function by encouraging undertakings to implement organisational, technical, and procedural safeguards before compromise occurs.

The preventive significance of reasonable steps is closely connected to the burden of proof in trade secret litigation. To establish the existence of a trade secret and demonstrate unlawful conduct, claimants must show that reasonable measures were adopted to preserve confidentiality (Würtenberger, 2019). In this sense, secrecy measures support both the substantive existence of the trade secret and the evidentiary credibility of the claimant's control over confidential information. Some authors nevertheless question whether the reasonable-steps requirement performs a genuinely evidentiary function, arguing that secrecy may also be established through alternative forms of proof (Bone, 2011, p. 16).

Ultimately, the analysis demonstrates that trade secret protection cannot be understood solely through the traditional logic of *ex post* private-law enforcement. Contemporary cyberthreats increasingly challenge the practical assumptions on which judicial enforcement depends, particularly attribution, detectability, and the restoration of secrecy after compromise. As a result, the effectiveness of trade secret protection increasingly depends upon broader systems of organisational resilience, cybersecurity governance, and preventive technological risk management designed to reduce vulnerability before misappropriation occurs.

4. The reasonable-steps requirement: between flexibility and cybersecurity governance

The institutional limitations discussed above help explain why the reasonable steps requirement under Article 2(1)(c) of the Trade Secrets Directive increasingly occupies a central position within contemporary trade secret protection. The challenges of detecting and attributing cyber misappropriation make preventive organisational and technical measures increasingly important for effective trade secret protection.

The Trade Secrets Directive requires that trade secret holders take reasonable steps to preserve confidentiality as a condition of protection. Unlike patents or other registered IPRs, trade secret protection is not automatic but contingent upon the holder's proactive conduct. At the same time, the Trade Secrets Directive deliberately refrains from defining what constitutes "reasonable steps", leaving their interpretation largely to national courts and future guidance from the Court of Justice of the European Union (Niebel, de Martinis and Clark, 2018, p. 449). This creates a flexible but inherently indeterminate standard.

4.1 Judicial interpretation and cybersecurity governance

Reasonable steps generally include legal and organisational measures, technical safeguards, and procedural controls (Aplin *et al.*, 2023, p. 832). Common examples include confidentiality agreements, restricted access systems, encryption, cybersecurity measures, employee training, and internal compliance procedures. Courts increasingly assess whether these measures are proportionate to the sensitivity and economic value of the information concerned.

Judicial interpretation remains highly contextual and fact-specific. Courts have consistently emphasised that trade secret protection does not require absolute secrecy or perfect technological security, but rather objectively reasonable measures in the circumstances (Higher Regional Court of Düsseldorf, 2021, para. 64). Relevant considerations typically include the economic value of the information, the size and resources of the undertaking, industry practices, and the foreseeability of particular risks (Hull, 2019, p. 37).

The comparative approaches discussed earlier in the article reveal important differences in how this standard is applied. German courts have

developed the most structured jurisprudence concerning reasonable secrecy measures, placing particular emphasis on organisational documentation, proportionality, and internal control systems (Munich Regional Court, 2019; Stuttgart Higher Regional Court, 2020). French courts continue to rely more heavily on flexible, fact-oriented balancing. In contrast, Estonian courts have adopted a comparatively formal, evidence-intensive approach that requires precise identification of the protected information and demonstrable secrecy measures. Nevertheless, courts generally accept relatively modest safeguards, such as password protection, restricted-access systems, or confidentiality agreements, provided that they are reasonably commensurate with the nature of the information and the resources of the undertaking (Cundiff, 2009; EUIPO, 2023, p. 36).

Importantly, neither the Trade Secrets Directive nor national jurisprudence requires compliance with specific cybersecurity frameworks or state-of-the-art technological solutions as a condition of protection. Trade secret law, therefore, remains distinct from cybersecurity regulation. Its purpose is not to guarantee technological invulnerability, but to determine whether the holder demonstrated a genuine intention to preserve confidentiality.

By contrast, some non-EU regimes adopt more formalistic approaches. Russian trade secret law, for example, requires the implementation of specifically enumerated protective measures before legal protection arises, thereby reflecting a more formalised and security-oriented approach to secrecy protection than the EU's flexible and context-dependent standard (Fox, 2020, p. 88). The Russian example is analytically relevant in part because contemporary cyber and intelligence activities targeting European technological innovation have increasingly been linked to Russian state-affiliated actors, making the comparison useful in illustrating how different legal systems conceptualise the relationship between secrecy, security, and organisational control.

Contemporary cyberthreats, however, increasingly challenge the assumptions underlying the reasonable-steps requirement. The concept was largely developed in the context of conventional commercial misappropriation involving employees, competitors, or contractual partners. Contemporary cyber operations operate differently. Automated extraction, advanced persistent threats, AI-assisted analysis, and state-linked cyber activities may circumvent even sophisticated organisational safeguards. Consequently, the distinction between reasonable protection and technological invulnerability becomes increasingly important.

4.2 Information security standards as evidentiary benchmarks

These developments have intensified discussion of the role of information security management standards, particularly ISO/IEC 27001, as potential benchmarks for assessing secrecy measures (ISO, 2022). Such standards are not legally binding, but they reflect internationally recognised approaches to information security governance, including access management, cryptography, incident response, and organisational accountability. Their practical relevance has also increased under the NIS2 Directive, which imposes risk-based cybersecurity obligations on essential entities.

Nevertheless, treating ISO/IEC 27001 certification or similar standards as *de facto* legal prerequisites for trade secret protection would fundamentally alter the structure of the reasonable steps requirement. Trade secret law has historically relied on flexibility and proportionality rather than formal technological compliance. Elevating cybersecurity standards to mandatory thresholds would risk privileging large, well-resourced undertakings while imposing disproportionate burdens on smaller entities and actors outside strategically sensitive sectors.

Accordingly, information security standards should be understood primarily as evidentiary indicators rather than determinative legal requirements. Compliance may demonstrate organisational diligence and cybersecurity maturity, but its absence should not automatically preclude protection. This approach preserves the contextual nature of the reasonable steps assessment while still allowing courts to account for evolving cyber risks when evaluating the adequacy of secrecy measures.

Geopolitical developments further complicate the assessment of what may reasonably be expected from trade secret holders. The Russian–Ukrainian war and the broader escalation of state-sponsored cyber activities targeting European technological assets illustrate how trade secret protection now intersects with questions of technological sovereignty, cybersecurity resilience, and strategic autonomy (Duguin and Pavlova, 2023; Peer and Baram, 2026).

4.3 Reverse engineering as a structural limit of trade secret protection

Even where undertakings implement extensive organisational and cybersecurity measures, trade secret protection remains subject to an important structural limitation: information lawfully obtainable through reverse engineering cannot generally remain protected once products are placed on the market. Article 3 of the Trade Secrets Directive explicitly recognises reverse engineering as a lawful means of acquiring information from a lawfully obtained product.

This reflects a fundamental distinction between trade secret protection and patent law. Whereas patent protection grants an exclusive right independent of secrecy, trade secret protection depends entirely on the continued maintenance of confidentiality. Once technological information becomes accessible through lawful analysis of a marketed product, secrecy-based protection may gradually erode regardless of the sophistication of prior organisational safeguards (Aplin, 2013).

The significance of reverse engineering extends beyond conventional commercial competition. In contemporary technological environments, reverse engineering may interact with automated analysis, AI-assisted inference, and large-scale technological extraction. This further illustrates that trade secret law cannot provide absolute control over strategically valuable technological information once such information becomes technologically observable or reproducible.

Yet reverse engineering restrictions could conflict with fundamental principles of IP law and competition policy. IP regimes intentionally distinguish between protected legal objects and unprotected functional ideas, technical principles, and publicly observable characteristics (Menell, Lemley and Merges, 2016). Limiting the use of lawfully reverse-engineered information would therefore risk creating *de facto* exclusivity beyond the traditional boundaries of trade secret protection. Even in exceptional circumstances, including armed conflict, such an expansion cannot be normatively justified.

These limitations are particularly relevant to dual-use technological innovation. In sectors where secrecy alone no longer provides sufficient protection against cyber-enabled extraction or reverse engineering, undertakings may increasingly rely on layered protection strategies combining trade secrets, cybersecurity governance, and selective patent

disclosure. The relationship between trade secret protection and selective disclosure, therefore, warrants closer examination.

5. Trade secrets and selective patent disclosure in contemporary cyber contexts

The preceding analysis demonstrates that trade secret protection remains an important but structurally limited mechanism for safeguarding strategically valuable technological innovation. Although trade secret law offers flexibility and potentially indefinite protection, its practical effectiveness increasingly depends on organisational resilience, cybersecurity governance, and the continued ability to maintain secrecy in environments characterised by cyber espionage, automated extraction, and attribution difficulties. These limitations become particularly significant in the context of dual-use technologies, where disclosure itself may create strategic vulnerabilities.

Traditionally, trade secrets and patents have been understood as alternative protection strategies: innovators either maintain secrecy or disclose inventions in exchange for exclusive patent rights. Contemporary cyber and geopolitical risks, however, increasingly complicate this binary distinction. In sectors involving strategically sensitive or dual-use technologies, secrecy alone may be difficult to maintain effectively, while full patent disclosure may expose commercially or strategically valuable information to adversarial actors.

5.1 Selective patent disclosure as a complementary protection strategy

In earlier research, the author proposed the concept of selective patent disclosure as a mechanism for limiting the exposure of strategically sensitive technological information within the patent system itself (Põld, 2025). Selective patent disclosure refers to deliberately limiting the information disclosed in a patent application or publication by withholding particularly sensitive technical details, such as specific methods, materials, or operational parameters, while preserving protection for other aspects of the invention.

The concept has increasing relevance in contemporary cyber environments. Published patent applications may reveal technological trajectories, industrial capabilities, and research priorities extending beyond

ordinary commercial competition (Van Caenegem, 2013). The growing use of automated patent analysis, AI-assisted inference, and large-scale technological monitoring further amplifies these risks. In sectors involving dual-use innovation, unrestricted disclosure may therefore create strategic vulnerabilities, particularly where effective enforcement against foreign or state-linked actors remains limited.

Selective patent disclosure should not be understood as an extension of trade secret protection or as an attempt to merge the two regimes into a unified framework. For example, the Court of Justice of the European Union has clarified that trade secrets cannot operate as a blanket justification for refusing access to information, requiring instead a balancing of the competing interests ('CK v. Dun & Bradstreet Austria GmbH', 2025). The mechanisms remain grounded in fundamentally different legal logics. Trade secret protection depends on the continued maintenance of secrecy, whereas patent protection presupposes disclosure as a condition of exclusivity. Once information enters the public domain through patent publication, it can no longer simultaneously function as a trade secret.

Accordingly, trade secrets and selective disclosure should instead be understood as complementary components within a layered innovation-protection strategy. Different elements of technological innovation may be protected through different mechanisms depending on their strategic value, vulnerability to reverse engineering, and exposure to cyberthreats. Commercial know-how, manufacturing processes, datasets, operational methods, and organisational practices may remain protected through trade secrecy and cybersecurity governance, while selected technical aspects capable of effective legal enforcement may be suitable for patent protection. The relationship between the two mechanisms is illustrated in Table 1.

As illustrated above, the choice between trade secret protection and patent disclosure is not merely doctrinal but a strategic assessment, and increasingly shaped by the surrounding threat environment. The growing prevalence of cyber-enabled extraction, difficulties in attribution, and automated technological analysis reduces the effectiveness of secrecy-based protection in isolation. At the same time, unrestricted patent disclosure may expose strategically valuable information to actors beyond the reach of effective legal enforcement mechanisms.

This does not imply that trade secret law should be replaced or that a separate *sui generis* regime for strategically sensitive innovation is required. Rather,

the analysis suggests that existing legal frameworks increasingly operate as interconnected components of a broader innovation-security architecture. Therefore, trade secret law, patent law, cybersecurity governance, and organisational risk management function less as isolated systems and more as complementary layers of technological protection.

Table 1. The relationship between trade secret protection and patent protection.

Criterion	Trade secret protection	Patent protection (including selective disclosure logic)
Legal basis	Strategic function	Exclusive right in exchange for disclosure
Core requirement	Information must remain secret and protected by reasonable steps	Full (or structured) disclosure of the invention
Strength of protection	Potentially indefinite but fragile	High, but time-limited (typically 20 years)
Vulnerability to cyberthreats	High, as secrecy can be compromised without detection or attribution	Medium: disclosure creates exposure, but rights remain enforceable
Dependence on enforcement	High, as requires detection and proof of misappropriation	High, but rights exist independently of secrecy
Suitability for dual-use technologies	More difficult to enforce effectively where threats are systemic and non-attributable	Problematic due to disclosure, but adaptable via selective disclosure
Risk profile	Loss is irreversible once secrecy is breached	Risk lies in strategic disclosure rather than loss of protection
Optimal use case	When secrecy can realistically be maintained, and threats are manageable	When enforcement is viable and controlled disclosure is acceptable
Strategic function	Defensive (preventing access)	Offensive and defensive (enabling control and signalling capability)

5.2 Towards a layered innovation-security framework

The analysis throughout this article suggests that traditional IP frameworks remain structurally oriented toward commercial environments characterised by identifiable actors, territorial enforcement, and legally attributable conduct. Contemporary cyberthreats operate differently. Automated extraction, AI-assisted inference, cross-border cyber espionage, and state-linked technological targeting increasingly challenge the assumptions underlying both trade secret and patent protection.

Trade secret law is particularly vulnerable to these factors because its effectiveness depends heavily on the preservation of secrecy, the detectability of misappropriation, and the availability of *ex post* enforcement. Once confidential information has been extracted through cyber operations or obtained through reverse engineering, legal remedies may provide only limited practical protection. Patent law, by contrast, offers stronger exclusive rights but simultaneously increases informational exposure through mandatory disclosure. In sectors involving dual-use technologies, both approaches therefore encounter important structural limitations when applied in isolation. This exposes a fundamental tension: IP law remains predominantly grounded in rights and reactive, whereas contemporary threats to technological innovation are systemic and call for preventive responses.

These developments suggest that the protection of strategically valuable innovation cannot be understood solely within the traditional boundaries of IP law. Instead, innovation protection increasingly depends on the interaction between private-law protection, cybersecurity governance, organisational resilience, and technological risk management.

Several practical implications follow. First, undertakings operating in strategically sensitive sectors should adopt layered protection strategies that combine trade secrets, cybersecurity governance, contractual safeguards, and selective patent disclosure, depending on the nature of the information concerned. Second, policymakers should avoid treating trade secret law as a self-sufficient solution to cyber-enabled technological extraction. Its institutional function remains narrower: it defines which confidential information warrants protection and provides remedies where unlawful conduct can be identified and attributed. Third, future discussion of selective patent disclosure should focus on developing proportionate, controlled disclosure mechanisms capable of addressing heightened security risks without undermining the fundamental structure of patent law.

The contemporary protection of dual-use technological innovation thus increasingly calls for an integrated innovation-security framework situated at the intersection of IP law, cybersecurity governance, and strategic technological resilience. Such an approach does not replace existing IP doctrines but instead recognises their institutional limits and complements them through broader systems of preventive technological governance.

6. Concluding remarks

This study demonstrates that, while EU trade secret law provides a flexible legal framework for protecting technological innovations, its effectiveness increasingly depends on proactive, preventive strategies. This does not indicate that trade secret law has failed as a legal doctrine. Rather, the analysis demonstrates that the institutional architecture of EU trade secret protection remains structurally oriented towards identifiable and attributable acts of commercial misappropriation, whereas contemporary cyberthreats increasingly operate through systemic, automated, and state-linked forms of technological extraction. In this respect, the article's original contribution lies in functionally mapping the core legal elements of trade secret protection—secrecy, reasonable steps, unlawful acquisition, and judicial enforcement—against contemporary cyberthreat environments. This mapping reveals a structural mismatch between the assumptions underlying traditional trade secret enforcement and the operational realities of contemporary cyber conflict.

Legal protection alone, particularly *ex post* remedies under Articles 10–14 of the Trade Secrets Directive, cannot adequately address sophisticated cyberthreats and state-level intelligence operations. The comparative analysis of Estonia, Germany, and France further illustrates that, despite formal harmonisation under the Trade Secrets Directive, national legal systems continue to differ in their evidentiary expectations, judicial reasoning, and approaches to organisational secrecy measures. Overall, while the three countries now share a common conceptual framework for trade secret protection derived from the Trade Secrets Directive, their legal traditions and distinct legislative approaches continue to shape the practical application of trade secret law. Estonia demonstrates a cautious, formal approach with limited jurisprudential development; Germany offers a highly systematised and jurisprudentially rich model; and France maintains a more flexible, case-specific approach despite codification.

The analysis further demonstrates that the practical effectiveness of trade secret protection increasingly depends on the integration of organisational resilience, cybersecurity governance, and preventive risk management into broader innovation-protection strategies, rather than on *ex post* judicial remedies.

Effective safeguarding of dual-use and strategically sensitive innovation requires an integrated approach that combines trade secret protection with organisational measures, robust cybersecurity governance, risk management, and selective patent disclosure. Selective patent disclosure complements trade secrets by providing controlled legal protection for specific aspects of an invention while minimising exposure of sensitive technical details.

Policymakers and enterprises should adopt layered protection strategies that align legal, technical, and procedural safeguards with organisational practices. Such an approach seeks to reconcile innovation incentives with strategic resilience, ensuring that knowledge assets remain both legally enforceable and operationally secure. For European organisations, this framework offers practical guidance, reinforcing the relevance of trade secret law while addressing contemporary technological and geopolitical challenges.

Ultimately, the article argues that contemporary protection of strategically relevant technological innovation cannot be understood solely within the traditional boundaries of IP law. Instead, trade secret protection must increasingly be conceptualised as part of a broader legal and institutional framework situated at the intersection of IP law, cybersecurity governance, and technological security.

Given the evolving nature of dual-use technologies, future research should pursue a more detailed and systematic examination of the legal and institutional mechanisms available for protecting intangible information.

Acknowledgements

The author would like to thank Prof. Aleksei Kelli and Prof. Irene Kull from the University of Tartu for their valuable input that enhanced the quality of this paper.

Lisette Põld is a PhD student and a junior research fellow in private law at the School of Law of the University of Tartu. Her research interests include intellectual property rights, and patent and trade secret protection.

References

Aplin, T. (2013) 'Reverse engineering and commercial secrets', *Current Legal Problems*, 66(1), pp. 341–377. Available at: https://doi.org/10.1093/clp/cut004

Aplin, T., Radauer, A., Bader, M.A. and Searle, N. (2023) 'The role of EU trade secrets law in the data economy: an empirical analysis', *IIC – International Review of Intellectual Property and Competition Law*, 54, pp. 826–858. Available at: https://doi.org/10.1007/s40319-023-01325-8

Bone, R.G. (2011) 'Trade secrecy, innovation, and the requirement of reasonable secrecy precautions', in R.C. Dreyfuss and K.J. Strandburg (eds) *The law and theory of trade secrecy: a handbook of contemporary research*. Edward Elgar Publishing, pp. 9–40. Available at: https://doi.org/10.4337/9780857933072.00010

Civil Code (France) 1804. Code civil. Légifrance, consolidated text. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721/ (Accessed: 17 January 2026).

'CK v. Dun & Bradstreet Austria GmbH' (2025) Case C-203/22. Judgement of the Court, 27 February. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-203/22 (Accessed: 23 January 2026).

Commercial Code (France) 1807. Code de commerce. Légifrance, consolidated text. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000005634379/2026-01-11 (Accessed: 18 January 2026).

Competition Act (Estonia) 2001. Konkurentsiseadus (KonkS). RT I, 18 November 2025, 2. Available at: https://www.riigiteataja.ee/akt/118112025002 (Accessed: 30 January 2026).

Constitution of the Republic of Estonia 1992. Eesti Vabariigi põhiseadus. RT 1992, 26, 349. Available at: https://www.riigiteataja.ee/akt/115052015002 (Accessed: 21 January 2026).

'Council directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' (2016) *Official Journal* L 157, pp. 1–18. Available at: http://data.europa.eu/eli/dir/2016/943/oj

Court of Cassation (France) (2025) Case No. 23-10.953. Judgement, 5 February. Available at: https://www.legifrance.gouv.fr/juri/id/JURITEXT000051151441 (Accessed: 18 January 2026).

Cundiff, V.A. (2009) 'Reasonable measures to protect trade secrets in a digital environment', *IDEA – The Intellectual Property Law Review*, 49(3), pp. 359–410. Available at: https://ipmall.law.unh.edu/sites/default/files/hosted_resources/IDEA/idea-vol49-no3-cundiff.pdf (Accessed: 18 January 2026).

Duguin, S. and Pavlova, P. (2023) *The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict*. European Parliament Think Tank Briefing. 4 September. Available at: https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594 (Accessed: 26 December 2025).

Employment Contracts Act (Estonia) 2008. Töölepingu seadus (TLS). RT I, 23 December 2024, 6. Available at: https://www.riigiteataja.ee/akt/123122024006 (Accessed: 30 January 2026).

EUIPO (2023) *Trade secrets litigation trends in the EU: IPR enforcement case-law collection*. EUIPO Publishing. Available at: https://www.euipo.europa.eu/en/publications/trade-secrets-litigation-trends-in-the-eu (Accessed: 3 January 2026).

Farkas, T. and Koch, P. (2016) 'The disclosure–fair trial dilemma when enforcing trade secrets in civil court proceedings', *Journal of Intellectual Property Law & Practice*, 11(12), pp. 901–909. Available at: https://doi.org/10.1093/jiplp/jpw153

Federal Labour Court (Germany) (2024) Case No. 8 AZR 172/23. Judgement of the Eighth Senate, 17 October. Available at: https://openjur.de/u/2499874.html (Accessed: 29 December 2025).

Fox, B. (2020) 'Tripping over the EU Trade Secret Directive: "reasonable steps" to get back on track', *Chicago-Kent | Journal of Intellectual Property*, 19(1), pp. 68–92. Available at: https://scholarship.kentlaw.iit.edu/ckjip/vol19/iss1/11 (Accessed: 15 December 2025).

Civil Code (Germany) 1896. Bürgerliches Gesetzbuch (BGB). *Bundesgesetzblatt*, consolidated text. Available at: https://www.gesetze-im-internet.de/bgb/ (Accessed: 19 December 2025).

Gougé, E. and Truchot-Bothner, A.C. (2019) 'The Trade Secrets Directive—France', *Les Nouvelles – Journal of the Licensing Executives Society*, 54(3), pp. 187–189. Available at: https://ssrn.com/abstract=3420351 (Accessed: 29 December 2025).

Higher Regional Court of Düsseldorf (2021) Case No. 15 U 6/20. Judgement of the 15th Civil Senate, 11 March. Available at: https://openjur.de/u/2363217.html (Accessed: 18 January 2026).

Higher Regional Court of Stuttgart (2020) Case No. 2 U 575/19. Judgement of the Second Civil Senate, 19 November. Available at: https://openjur.de/u/2348225.html (Accessed: 29 December 2025).

Hoeren, T. (2018) 'The EU Directive on the protection of trade secrets and its relation to current provisions in Germany', *Journal of Intellectual Property, Information*

Technology and Electronic Commerce Law, 9(2), pp. 138–145. Available at: https://www.jipitec.eu/jipitec/article/view/223 (Accessed: 22 December 2025).

Hull, J. (2019) 'Protecting trade secrets: how organisations can meet the challenge of taking "reasonable steps"', *WIPO Magazine*, 1 October, pp. 35–39. Available at: https://www.wipo.int/en/web/wipo-magazine/articles/protecting-trade-secrets-how-organizations-can-meet-the-challenge-of-taking-reasonable-steps-41043 (Accessed: 18 January 2026).

ISO (2022) *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. International Organization for Standardization. Available at: https://www.iso.org/standard/27001 (Accessed: 30 January 2026).

Labour Code (France) 1910. Code du travail. Légifrance, consolidated text. Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072050/ (Accessed: 17 January 2026).

Law of 30 July 2018 on the protection of trade secrets (France) 2018. Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. Légifrance. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111 (Accessed: 18 January 2026).

Law of Obligations Act (Estonia) 2001. Võlaõigusseadus (VÕS). RT I, 11 November 2025, 16. Available at: https://www.riigiteataja.ee/akt/111112025016 (Accessed: 30 January 2026).

Law on the Protection of Trade Secrets (Germany) 2019. Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). *Bundesgesetzblatt*, consolidated text. Available at: https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html (Accessed: 19 December 2025).

Menell, P.S., Lemley, M.A. and Merges, R.P. (2016) *Intellectual property in the new technological age: 2016—Chapters 1 and 2*, Stanford Public Law Working Paper, No. 2780190. Available at: https://doi.org/10.2139/ssrn.2780190

Niebel, R., de Martinis, L. and Clark, B. (2018) 'The EU Trade Secrets Directive: all change for trade secret protection in Europe?' *Journal of Intellectual Property Law & Practice*, 13(6), pp. 445–457. Available at: https://doi.org/10.1093/jiplp/jpx227

Ohly, A. (2020) 'Germany: the Trade Secrets Protection Act of 2019', in J. Schovsbo, T. Minssen and T. Riis (eds) *The harmonisation and protection of trade secrets in the EU*. Edward Elgar Publishing, pp. 103–123. Available at: https://doi.org/10.4337/9781788973342.00012

Peer, N. and Baram, G. (2026) 'Blurred lines: the expanding role of the private sector in wartime cyber operations—the case of the Russia–Ukraine war', *Cyber Security: A Peer-Reviewed Journal*, 9(3), pp. 239–254. Available at: https://doi.org/10.69554/PPXU2105

Põld, L. (2025) 'Patent disclosure vs technological security: balancing Western innovation protection in a geopolitical conflict', *International Comparative Jurisprudence*, 11(1), pp. 32–46. Available at: https://doi.org/10.13165/j.icj.2025.11.004

Rantasaari, K. (2023) 'Patent litigation in Europe: intermediate fee shifting and the UPC', *Journal of Intellectual Property Law & Practice*, 18(9), pp. 642–654. Available at: https://doi.org/10.1093/jiplp/jpad063

Regional Court of Munich I (2019) Case No. 7 O 3890/19. Order of 13 August. Available at: https://openjur.de/u/2275835.html (Accessed: 29 December 2025).

Restriction of Unfair Competition and Protection of Business Secrets Act (Estonia) 2018. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (EKTÄKS). RT I, 7 December 2018, 2. Available at: https://www.riigiteataja.ee/akt/107122018002 (Accessed: 30 January 2026).

Riis, T. and Schovsbo, J. (2019) 'To be and not to be an IPR—the protection of trade secrets in the EU', *European Intellectual Property Review*, forthcoming. University of Copenhagen Faculty of Law Research Paper No. 2019-71. Available at: https://doi.org/10.2139/ssrn.3347705

Rutiku, S. (2025) 'Akadeemiline vabadus ja teadusjulgeolek on lahutamatud' [Academic freedom and research security are inseparable], *ERR*, 23 November. Available at: https://www.err.ee/1609862760/siret-rutiku-akadeemiline-vabadus-ja-teadusjulgeolek-on-lahutamatud (Accessed: 22 December 2025).

Schröder, V. and Widera, P. (2021) 'Obtaining evidence in patent litigation and trade secret protection—a tale of two poles', *GRUR International*, 70(4), pp. 361–376. Available at: https://doi.org/10.1093/grurint/ikaa161

Supreme Court of Estonia (2009) Case No. 3-1-1-46-09. Judgement of the Criminal Chamber, 8 June. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-46-09 (Accessed: 20 December 2025).

Supreme Court of Estonia (2020a) Case No. 1-18-4590. Judgement of the Criminal Chamber, 15 May. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=1-18-4590/82 (Accessed: 20 December 2025).

Supreme Court of Estonia (2020b) Case No. 2-19-9918. Judgement of the Civil Chamber, 21 October. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=2-19-9918/31 (Accessed: 20 December 2025).

Unfair Competition Act (Germany) 2004. Gesetz gegen den unlauteren Wettbewerb (UWG). *Bundesgesetzblatt*, consolidated text. Available at: https://www.gesetze-im-internet.de/uwg_2004/BJNR141400004.html (Accessed: 19 December 2025).

Van Caenegem, W. (2013) *Trade secrets and intellectual property: breach of confidence, misappropriation and unfair competition*. Kluwer Law International. Available at: https://tind.wipo.int/record/27344 (Accessed: 23 January 2026).

Van Dijk, N. (2017) 'Legal theory: from intellectual property to informational goods', in N. van Dijk (ed) *Grounds of the immaterial: a conflict-based approach to intellectual rights*. Edward Elgar Publishing, pp. 5–32. Available at: https://doi.org/10.4337/9781786432506.00007

Varadarajan, D. (2014) 'Trade secret fair use', *Fordham Law Review*, 83(3), pp. 1401–1454. Available at: https://ir.lawnet.fordham.edu/flr/vol83/iss3/9 (Accessed: 3 January 2026).

Värv, A. (2020) 'Ärisaladuse kaitse uus nägu' [The new face of trade secret protection], *Juridica*, 5, pp. 419–428.

Värv, A., Pisuke, H., Mets, T., E. Vasamäe and Kelli, A. (2010) 'Trade secrets in the intellectual property strategies of entrepreneurs: the Estonian experience', *Review of Central and East European Law*, 35(5), pp. 315–339. Available at: https://doi.org/10.1163/157303510X12650378240476

Würtenberger, G. (2019) 'Protection of trade secrets and know-how in the European Union: the EU Trade Secrets Directive (EU) 2016/943', *IP-Iurisdictio*. Available at: https://ip-iurisdictio.org/protection-of-trade-secrets-and-know-how-in-the-european-union-the-eu-trade-secrets-directive-eu-2019-943/#_ftn23 (Accessed: 11 January 2026).