International Comparative Jurisprudence 2025 Volume 11 Issue 1
ISSN 2351-6674 (online) DOI: https://doi.org/10.13165/j.icj.2025.11.004

PATENT DISCLOSURE VS TECHNOLOGICAL SECURITY: BALANCING WESTERN INNOVATION PROTECTION IN A GEOPOLITICAL CONFLICT[1]

Lisette Põld [2]
University of Tartu, Estonia.
Email: lisette.pold@ut.ee

Received: 31 March 25; accepted: 19 May 2025
DOI: https://doi.org/10.13165/j.icj.2025.11.004

Abstract. Innovation is pivotal in national economic development, and it is essential that intellectual property (IP) rights are protected. Geopolitical tensions, especially since the beginning of the Russia-Ukraine war, highlight the need to safeguard Western technological innovation. Despite sanctions aiming to restrict Russia's access to advanced technology, Russia circumvents restrictions and deliberately violates Western IP rights. This article explores the limitations of existing technological sanctions and proposes a reform to the patent system by considering selective disclosure for dual-use technology patent applications. Selective disclosure of a patent application would provide key strategic benefits to Western nations in protecting their technological innovation and IP rights while maintaining the core principles of IP protection. This approach balances technological security with open innovation, ensuring that only trusted entities have controlled access to critical technological information.

Keywords: Patents, Invention Secrecy, Intellectual Property, Sanctions, Patent Disclosure.

Introduction

Protecting Western[3] technological innovation has become a critical priority in recent years amid growing geopolitical tensions, particularly with Russia. The war in Ukraine is unfolding across multiple fronts, including economic ones such as technological warfare. As a result of the European Union (EU) sanctions imposed on Russia in response to its aggression against Ukraine, the safeguarding of cutting-edge innovations, from artificial intelligence (AI) and cybersecurity systems to sensitive intellectual property (IP), has emerged as a central concern for governments, companies and institutions alike.

Russia's economy has historically depended on Western technology in a variety of sectors, although the degree of reliance has varied. Before Russia invaded Ukraine on 24 February 2022, the EU was Russia's largest trading partner, while Russia was the EU's fifth-largest trading partner, with significant trade in energy and machinery (European Commission, 2024a). Key areas in which Western technology has played an important role in Russia's economy include aerospace, defence, and information and digital technology (Marcus et al., 2022; Sherman, 2024).

Through the sanctions imposed so far, the EU has reduced bilateral trade flows with Russia and introduced restrictions on the transportation and export of technology, machinery components and electronic goods (European Council, n.d.). Sanctioned goods include software for drones and encryption devices, electronic components used in weapons systems, specialised materials and industrial machinery. The purpose is to target sensitive sectors in Russia's military-industrial complex and limit

[1] The author would like to thank Prof Aleksei Kelli from the University of Tartu for his valuable input that enhanced the quality of this paper.
[2] Junior Research Fellow in Private Law at the University of Tartu.
[3] In this paper, 'the West' and 'Western countries' are interchangeable terms, used to denote democratic, market-economy industrialised countries, predominantly the member states of the EU and NATO.

the country's access to critical advanced technology (European Commission, n.d.). The EU has also urged other countries,[4] including European allies, to align with its restrictive measures and broader normative framework (Renda, 2023).

Restrictive measures have been partly successful in curbing Russia's military activity, as evidenced by Russia's problems in producing innovative military equipment, including aircraft and munitions (Orlov, 2024). However, at the same time, Russia is increasingly seeking economic relations with other countries, such as China, Kazakhstan, Türkiye and countries in the Middle East (Mosolova & Fleming, 2023; Kolyandr 2024). Russia has been known to leverage Western technologies across sectors. The inflow of new Western technology represents a strategic interest for Russia. Meanwhile, Russia's geopolitical objectives pose a threat to Western technological security and the enforcement of IP rights.

Sanctions are one tool that can be used to address such crises, but unconventional and multidimensional solutions should also be explored. One possible tool to protect Western technological innovation is to reform the traditional patent system by adopting a selective disclosure approach. This means not disclosing in patent databases the technical description of a patent application involving dual-use technology, i.e. technology that has potential applications for both civil and military purposes. However, this raises concerns about the patent system's functioning, open innovation, disclosure requirements and public access to patent information.

This article delves into the challenges of protecting Western technology from Russian threats through the lens of patent law, focusing on selective disclosure in patent law as a tool to safeguard innovations. It explores the intersection of dual-use technology, technological security and intellectual property, analysing how EU technology sanctions can be circumvented and the implications for dual-use technologies. By proposing limits on patent disclosure to prevent misuse by hostile actors, the article offers a comprehensive approach to balancing transparency with security in the protection of Western technological innovations.

I rely on traditional legal methods such as the analytical method, analysing the EU's legal doctrine and legislation alongside examples from German, Estonian, Latvian and Lithuanian law. I also draw data from books, articles, legislation, journals, reports and other publications related to the research topic. AI-assisted technology was used in the preparation of this article for checking grammar and spelling. The core analysis and insights, however, are solely those of the author.

1. Technology, IP and Sanctions in the Russia-Ukraine War

Since March 2014, the EU has progressively imposed restrictive measures (sanctions) against Russia. Sanctions were expanded following Russia's military aggression against Ukraine in February 2022. A significant step in strengthening these sanctions occurred on 25 February 2022, when the EU adopted Regulation (EU) 2022/328. This regulation amended Council Regulation (EU) 833/2014, introducing a comprehensive ban on exporting dual-use items to Russia. The EU has progressively imposed extensive sanctions targeting Russia's military-industrial complex, restricting access to advanced software, encryption devices and key electronic components (European Commission, n.d.). These restrictions include dual-use components regulated under allied export controls, such as optical systems used in manufacturing, bearings for moving vehicles, machine tools in the military and weapons industry, aircraft engines, and microchips (Bergmann et al., 2023).

EU sanctions against Russia are implemented through a two-step legal mechanism: Council Decisions and Council Regulations. Council Decisions, under the Common Foreign and Security Policy (CFSP), are based on Article 29 of the Treaty on European Union (TEU). Their purpose is to establish the political and strategic framework for sanctions, such as targeting certain sectors or individuals. These Council Decisions are binding on EU member states, but they do not have any direct effect on individuals or

[4] These countries include EU membership candidates and potential candidate countries, European Economic Area states and European Free Trade Association states.

companies. Council Regulations are based on Article 215 of the Treaty on the Functioning of the European Union (TFEU). Their purpose is to give practical effect to Council Decisions, e.g. freezing assets and restricting exports. Regulations are directly binding and applicable in all EU member states, and they apply automatically without the need for national implementation of legislation. In short, Council Decisions are politically binding on EU member states, not individuals or companies, while Council Regulations are legally binding on individuals and companies.

The EU's sanctions have widened Russia's technological gap with the West, forcing it to abandon its original technological advancement plans and shift focus to replicating foreign technology. This shift became evident when Russia gave up on its technological development strategy for 2030, which aimed for progress in key areas such as hydrocarbon processing equipment, the aviation industry, air transport infrastructure, and power engineering (Petrova & Sapozhkov, 2023). Instead of leading in innovation, Russia is now primarily engaged in damage control, relying on reproducing existing foreign technologies (Epifanova, 2023).

EU regulations, such as Article 2(1) of Regulation (EU) 833/2014, prohibit the sale, supply, transfer or export of dual-use goods and technology to Russia or for use there if these items are intended for military use or a military end-user, regardless of their origin. Articles 4(1)c and 4(1)d prohibit the provision of technical assistance, brokering services or financial support for dual-use goods and technology to Russia or for use there if intended for military use or a military end-user. According to Article 1a of Regulation (EU) 833/2014, dual-use goods and technology are the items listed in Annex I to Regulation (EC) 428/2009.

The EU has recently implemented several measures to enhance the enforcement of sanctions against Russia, with a particular focus on dual-use goods and advanced technologies critical to Russia's military capabilities. In October 2023, the European Commission issued a list of economically critical goods subject to EU sanctions, helping businesses and third countries prevent circumvention. The European Council's February 2024 Common High Priority Items list further targets advanced technological components used for military applications. The list encompasses 50 customs codes, aiding exporters in compliance and assisting enforcement agencies in preventing circumvention of sanctions. Specifically, the list comprises particular dual-use goods and advanced technology items, such as central processing units, electronic integrated circuits, and machinery parts, essential for developing, producing or using Russian military systems. These measures increase exporter compliance and assist customs and enforcement agencies in combating illegal technology transfers (European Commission, 2024b).

The 14th EU sanctions package against Russia, adopted in June 2024, is a set of legally binding restrictive measures established under the EU's CFSP framework. These measures are enforceable across all EU member states and are directly applicable to individuals, businesses and organisations under EU jurisdiction. They aim to curb sanction evasion by imposing due diligence requirements on EU businesses (European Commission, 2024c).

Consequently, companies must ensure that industrial know-how and battlefield goods do not reach Russia via third-country subsidiaries. EU operators exporting dual-use technology must implement compliance mechanisms to identify and mitigate the risk of re-exportation to Russia (European Council, 2024). Additionally, contractual obligations must prevent transferred knowledge from being exploited for military purposes (European Council, n.d.). In the case of a violation, an EU company must report the breach to the relevant national authority in the member state where they are registered or reside (European Council, n.d.). Therefore, EU parent companies must ensure that their third-country subsidiaries do not participate in any activities that result in an outcome that the sanctions seek to prevent.

Emerging technologies offer Russia a means with which to challenge Western dominance and IP protections. For instance, NATO (the North Atlantic Treaty Organization), concerned about safeguarding IP (Herzog & Dominika, 2024), has enlisted partners such as the Estonian technology firm Nortal (Trade with Estonia, 2025) to counter these threats. However, NATO members vary in their

commitment to sanctions. Türkiye, for example, has not imposed sanctions and continues trade relations with Russia, posing a risk of circumvention (Scazzieri, 2024; European Commission, 2023). Furthermore, many sanctioned components, such as chips, electronic circuits and industrial machinery, continue to reach Russia via Central Asia and the Middle East (Murilo Rangel Da, 2025).

The dual-use nature of many technologies further complicates enforcement. Furthermore, enforcing these sanctions is complex due to inconsistent application across EU member states and loopholes in international trade (Giumelli, 2024). Russia exploits shell companies and legal gaps to acquire restricted goods, complicating global enforcement efforts (Feldstein & Brauer, 2024). For instance, there are reports of Russian weapons filled with Western technological components (Shagina, 2023), while reports indicate that in 2023, nearly half of all Russian battlefield imports originated from Western multinational corporations operating through third-country intermediaries (Rooke, 2024).

Multinational corporations with subsidiaries in non-sanctioned countries, such as China, Hong Kong and the United Arab Emirates, inadvertently contribute to sanction circumvention (Rooke, 2024). Given that multinational corporations operate across multiple jurisdictions, the intricate dynamics of supply chain logistics obscure the destination of critical and high-priority technology. It is doubtful that the EU can extend its policy to ban trade with Russia by non-EU-based subsidiaries owned or controlled by EU companies.

Meanwhile, Russia compensates for technological shortfalls by acquiring Western technology and equipment through black-market channels, increasing industrial espionage and IP theft. One of Russia's key vulnerabilities is its dependence on imports of sensitive technology. It has been noted that the Russian government and courts have been undertaking actions to illegitimately deprive EU member state IP rights holders of their protection in Russia (Recital 20 of the Council Decision (CFSP) 2024/1744). In particular, on 6 March 2022, the Russian Federation passed a decree allowing local companies and individuals to use the inventions, utility models and industrial designs of patent holders from 'unfriendly countries' (Decree No. 430-p) without their consent and with no compensation (Decree No. 299). Russia implemented this measure as a sanction against the West.

Additionally, on 29 March 2022, Russia introduced a parallel import mechanism, legalising the importation of certain foreign products without the manufacturer's approval (Order No. 1532). In June 2024, Russia announced plans to make this measure permanent.(Interfax, 2024). Russia aims to continue violating Western IP rights even once its war with Ukraine ends, seeking foreign technology it cannot produce itself. Patent information for such inventions is valuable to Russia's technology experts.

The EU has responded by restricting IP protections for Russian entities. Under Regulation (EU) 833/2014, implemented in June 2024, Article 5s prohibits EU IP offices from accepting applications for trademarks, patents, designs, utility models or geographical indications from Russian nationals, residents or entities. This measure covers applications filed with national EU patent offices, the European Patent Office and the World Intellectual Property Organization (WIPO). As a result, Russian companies and individuals are unable to prevent EU companies and individuals from using their innovations in the EU because they will not be granted a patent and will be excluded from IP protection.

European IP offices must now identify and suspend such applications by cross-referencing them against sanctioned entities listed in Annex I of Regulation (EU) 269/2014. When processing applications, the European Commission, the EU Intellectual Property Office (EUIPO) and national IP offices may request additional proof of nationality and residency (European Commission, 2024d). Additionally, a non-official consolidated list of sanctioned names and entities is available on the EU sanctions map[5] and in the financial sanctions database.[6] Although formal refusals are not mandated (Recital 20 of the Council Decision (CFSP) 2024/1744), IP offices are instructed to flag affected entries in their databases as frozen due to EU sanctions rather than removing them (European Commission, 2024d).

[5] See: EU sanctions map. https://www.sanctionsmap.eu/# (accessed 19 January 2025).
[6] See: Financial sanctions database. https://webgate.ec.europa.eu/fsd/fsf#!/files (accessed 19 January 2025).

The contrasting approaches of the EU and Russia in IP protection reflect broader geopolitical tensions. While the EU seeks to prevent Russia from accessing advanced technology and to protect IP rights, Russia's Decree No. 299 facilitates the unauthorised use of Western patents and trademarks. This struggle highlights the strategic importance of IP in modern conflicts, as nations leverage technology and legal frameworks to either enforce or undermine innovation protections in times of geopolitical crisis. However, balancing transparency with security remains a key challenge.

2. Balancing Patent Disclosure, Technological Security and Innovation Protection

2.1. Role of the Disclosure Requirement in the Patent System

A patent is a legal right granted to an inventor, providing exclusive rights for a limited period, typically 20 years from the date of filing the patent application. The patent system operates on a fundamental principle of disclosure, requiring applicants to publicly share details of their inventions through a written document known as a patent application.

The disclosure requirement serves multiple purposes, including promoting knowledge dissemination, preventing duplication and incentivising innovation. While the patent owner retains the right to exclude others from using the invention until the patent expires, the technical information disclosed in the application holds considerable value for the public (Seymore, 2010). Others are free to use the information, provided they do not infringe upon the patent owner's rights.

The scope of a patent is defined by the application documents and is governed by the Agreement on Trade-Related Aspects of Intellectual Property Rights (hereinafter referred to as the TRIPS Agreement). Article 28(1) of the TRIPS Agreement grants patent owners the right to prevent others from making, using, selling or importing the patented product (1a) or using a patented process and its directly obtained product (1b) without consent. Article 28(2) also allows patent owners to transfer or license their patents.

To obtain a patent, an inventor must provide a clear and complete description of the invention, ensuring that a person skilled in the field would be able to replicate it (Rantanen, 2013). Article 29 of the TRIPS Agreement mandates that applicants disclose their inventions thoroughly, potentially requiring them to indicate the best known mode for carrying out the invention when filing. For instance, the Estonian Patents Act § 19(1) states that a patent application must disclose the invention sufficiently clearly and concisely to enable replication by a skilled person. Similar provisions exist in German (Patent Act Section 34(3-4)), Lithuanian (Patent Law Article 16) and Latvian (Patent Law Section 30(1)) legislation.

Patent information is made publicly accessible through various patent databases maintained by national IP offices.[7] If an application is denied, its details are still made publicly available. If granted, both the patent and the complete legal documentation involved in securing it are disclosed (Beckerman-Rodau, 2009). For example, under Estonian law (§ 35(3) of the Patents Act), the Estonian Patent Office registers granted patents and publishes their details. In Germany, the German Patent and Trademark Office publishes an application's first publication, patent specifications and entries in the Patent Gazette (Patent Law Sections 32(1), 32(3) and 58(1)). Similarly, in Lithuania and Latvia, their national patent offices publish patent descriptions, claims and drawings upon granting a patent (Lithuanian Patent Law Articles 28(5) and 29(1); Latvian Patent Law Section 35(2-3)).

The disclosure principle forms a *quid pro quo* arrangement: in exchange for exclusive rights for a limited period, inventors share their knowledge with the public, fostering further innovation (Devlin, 2010). Therefore, patents are intended to communicate information about an invention to the public and encourage innovation. However, some argue that this assumes that detailed technical disclosure is a central purpose of the patent system (Burk, 2016). The focus is placed on the notion that disclosure is

[7] A comprehensive list of national patent databases is available at https://www.epo.org/en/searching-for-patents/technical/espacenet/national (accessed 5 February 2025).

integral to the patent system, either as a primary objective or as a policy goal reinforced by judicial decisions.

When national security concerns arise, the emphasis on disclosure introduces complexities. While patents promote innovation through public knowledge-sharing, publishing sensitive technologies, especially those with dual-use applications, can pose security risks. Such disclosures may reveal critical technological details to foreign adversaries or hostile actors.

Patent applications are written in technical language, targeting experts in the relevant field rather than the general public (Burk, 2016). This practice originated in the 19th century, when industrial economies were relatively small, and few individuals outside the technical domain encountered patent-related issues (Janis & Holbrook, 2012). In modern times, patents remain primarily addressed to skilled professionals (Burk, 2016). This raises the question of whether the disclosure requirement genuinely serves broader public knowledge or mainly facilitates communication within technical communities. It has been pointed out that proving which legal information about patents is transmitted to the lay public may be too difficult (Janis & Holbrook, 2012). Therefore, while patent information can aid technological transfer, some argue that it is one of the lesser functions of disclosure (Burk, 2016).

Consequently, disclosure should be considered a secondary rather than a primary goal of the patent system. The patent system does not completely prevent the withholding of information, which could limit public knowledge. On the contrary, IP laws encourage innovation and commercialisation of technology rather than merely providing public information (Devlin, 2010). In cases involving dual-use technologies, withholding specific technical details may be justified for national security reasons.

While reverse engineering may give rise to obtaining information not disclosed in patent databases, it is argued that an invention's disclosed specifications can instantly provide more of the same information that could be obtained through reverse engineering the invention (Devlin, 2010). While limiting disclosure might undermine the open exchange of knowledge, especially in fields where innovation builds on prior inventions, such a limitation could be considered a necessary compromise to balance public safety and technological advancement with the protection of sensitive technologies.

Restricting certain disclosures must be carefully managed to balance transparency and innovation without compromising security. Selective disclosure of sensitive inventions does not fundamentally undermine the patent system's purpose, as access to restricted information can still be requested through controlled channels. If managed effectively, with clear guidelines for dual-use technologies, innovation can be protected without significantly hindering the patent system's broader objectives. Therefore, while disclosure plays a crucial role in the patent system, its function should be viewed in a nuanced manner. Although it facilitates knowledge-sharing, its primary aim remains to protect and commercialise technological advancements.

2.2. Innovation and the Security of Technological Know-how

Strategic information extends beyond military activities to include patents, as anything relating to a nation's security can be considered strategic. Patents involving innovative or sensitive technology are key sources of strategic information, especially for technologies with dual-use applications, e.g. advanced materials, cybersecurity software, AI and biotechnologies.

Concerns around the protection of IP and technological innovations raise the question of whether the traditional principle of full disclosure in patent law should be re-evaluated. Historically, disclosing patent details has been seen as a core function of the patent system, promoting transparency and innovation. Regarding the Russia-Ukraine war, public disclosure could inadvertently provide foreign governments, foreign organisations or hostile actors access to technologies that could be weaponised or used to undermine a nation's defence or economic security.

The intersection of patent law and national security becomes crucial here. NATO member states, including many European countries, have implemented secret patent systems to protect sensitive technologies, such as military innovations and critical infrastructure solutions (Põld, 2024). These inventions remain undisclosed in patent databases to safeguard national security, economic interests or foreign policy objectives. A risk arises from the potential misuse of publicly disclosed technologies, which foreign actors could reverse-engineer or exploit, especially during heightened geopolitical tensions, such as the ongoing Russia-Ukraine conflict.

Estonia's Patents Act Section 24(4) mandates that classified patent applications are not published in the patent register. Sections 19(4) and 19(5) specify that patents related to national defence or considered to be such by a foreign government through international agreements can be classified. Germany's Patent Act Section 50(1) requires that if a patent concerns a state secret, no publication of the invention can be made. The German Criminal Code Section 93 defines state secrets as information that must remain confidential to protect the nation's external security.

Lithuania's Patent Law Article 27(3) stipulates that access to secret inventions must follow a prescribed legal process. Additionally, Article 26(5) ensures that inventors receive compensation for classified inventions related to national defence. Latvia's Patent Law Section 11 offers a more transparent approach to secret inventions. It allows the Ministry of Defence to designate an invention as secret if it pertains to national defence interests, and it excludes specific provisions regarding the publication of patent applications and registration.

Patents are territorial, meaning they are only enforceable within the jurisdiction where they are granted. For global protection, inventors must apply for patents in multiple jurisdictions. This territorial nature calls for international measures to secure Western technologies, as regional sanctions alone may not be sufficient. As national patent systems are rooted in international agreements, such as the European Patent Convention (EPC) and the TRIPS Agreement, reform must be conducted in the global patent system.

One proposed solution is to restrict the disclosure of certain information within patent applications, particularly the details of dual-use technologies. Instead of fully disclosing these details, the patent system would adopt a model of selective disclosure, where only trusted parties, based on security priorities, are granted access to the complete documentation of sensitive inventions. The proposal suggests that technological innovation can be better protected by restricting access to the technological description of certain types of dual-use technologies.

IP rights are a key policy tool for controlling the distribution of knowledge across systems. The OECD defines innovation as 'a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by the unit (process)' (OECD, 2018, p 20). Open innovation is a concept where organisations use external and internal ideas, knowledge and resources to accelerate the development of their products or services (De Beer, 2021).

The patent system is generally considered a policy tool to foster innovation (Ponchek, 2016). Patents can be a source of innovation, but their role is more indirect. Patents can facilitate open innovation by disclosing technical information to the public, using exclusion to stimulate innovation. However, the relationship between patents and innovation varies by industry sector and an individual firm's characteristics (OECD, 2008). This does not necessarily mean that the information used for cumulative innovation resides exclusively or predominantly within the confines of patent specifications (Devlin, 2010). Also, evidence shows that most inventors rarely read others' patents and rank patents last as a source of innovation, often due to concerns about infringement, difficulty with legal jargon, or the limited information patents provide (Anderson, 2011).

Open innovation relies on the premise that shared knowledge leads to collaborative progress (Bogers, 2012). Despite this, research shows that many patented inventions never become innovations, and many innovations are never patented (De Beer, 2021). If key technical descriptions of dual-use technologies

are non-disclosed, it could slow innovation in some areas, as other inventors and researchers would be unable to access or build upon this knowledge (e.g. the case of secret patents). However, if an option exists to apply for access to the technological know-how, it is not an absolute non-disclosure. In this case, the measure will not severely affect the dissemination of knowledge because the invention will not be excluded from the public.

One can conclude that society is better off with a patent system that incentivises invention and commercialisation without requiring disclosure than with a system that dilutes *ex ante* incentives and reduces the incidence of invention by demanding as much disclosure as possible (Devlin, 2010). Therefore, regarding the Russia-Ukraine war, society should prioritise limiting disclosure over maximising it to protect Western technological innovation and technical know-how.

3. The Disclosure Requirement Limitation: The Case for Selective Disclosure of Dual-Use Technologies

3.1. Absolute Non-disclosure of a Patent Application

Finding the right balance between transparency and technological security requires careful consideration. Excessive secrecy could undermine the fundamental purpose of the patent system, limiting public access to valuable technological knowledge. Conversely, too much transparency could expose sensitive information to adversaries, jeopardising national defence capabilities. This balance must continuously evolve as new technologies emerge and security threats shift, necessitating ongoing adaptation of patent policies and legal frameworks to safeguard public innovation and national security interests.

Patent ownership rights generally stem from an invention's creator or legal agreements governing an invention. Patents are considered intangible personal property (Beckerman-Rodau, 2009). Secret patents, particularly those originating from NATO agreements, withhold patent rights and prohibit disclosure to prevent technology from being transferred to foreign adversaries. Given the trade-offs between national security concerns and the benefits of open innovation, expanding the concept of secret patents to cover all dual-use technologies is not feasible.

Applying secret patents to all dual-use technologies would create a closed innovation paradox, wherein innovation activities occur exclusively within a single organisation (Leminen et al., 2015). This could discourage companies from seeking external ideas or collaborating with outside entities. Closed innovation involves internal strategies for acquiring and commercialising technology, but a secret patent system would restrict the broader community from benefiting from disclosed technological advancements. Technological progress may be delayed without public access to a significant portion of patent information, as inventors could not build upon existing patents to drive further advancements or improvements.

A key reason why expanding secret patents to all dual-use inventions is impractical is the issue of compensation. Secret patents prevent inventors from fully commercialising their inventions, necessitating compensation for lost commercial opportunities. Under the current patent system, Article III of NATO's Agreement on Mutual Safeguarding of the Secrecy of Defense-Related Inventions ensures that if a government enforces secrecy on a defence-related invention to protect national security, the inventor cannot later demand compensation for any harm caused by the secrecy. This system balances national security concerns with an inventor's rights by ensuring the inventor receives compensation from the entity imposing secrecy.

National patent laws establish compensation criteria, yet details around how the amount of compensation is calculated remain opaque. Typically, the amount of compensation results from an agreement between an inventor and the entity enforcing secrecy, usually the government. For example, under Section 55(1) of the German Patent Act, compensation is assessed based on factors such as the economic situation of the affected party, the expenses incurred in developing or acquiring rights to the

invention, the likelihood that secrecy would be necessary at the time of development, and any benefits the affected party derives from alternative uses of the invention.

Similarly, Estonia's Patents Act § 18^1(2) considers the estimated service life of a classified invention and the commercial profit that the patent owner would likely have earned if the invention had not been classified. Latvia's Patent Law Section 11(3) states that if the patent owner and the Ministry of Defence cannot agree on compensation, the court will determine the amount based on the procedure outlined in the Latvian Civil Procedure Law.

The current compensation system functions effectively because the number of secret invention cases is limited, and governments assume financial responsibility as the restricting entity. However, expanding the secret patent system to all dual-use technologies presents significant challenges.

A compensation system covering all dual-use technologies would be unworkable due to the sheer scale of payments required and the absence of a precise mechanism to determine financial responsibility. With civilian and military applications feasible across various industries, dual-use technologies would generate overwhelming financial obligations if restricted under a secret patent system. Governments would have to allocate enormous funds to compensate inventors, an approach likely to be unsustainable.

Unlike national security-related inventions, where the government is the clear stakeholder, dual-use technologies serve public and private interests. Expecting governments to cover all compensation costs would be unrealistic, while mandating private sector contributions would create legal and economic complexities. Additionally, restricting the commercialisation of a vast range of inventions would disrupt industries, deter private-sector innovation and reduce incentives for R&D investment. Companies anticipating that their patents might be classified as secret and their compensation uncertain could be discouraged from developing critical technologies. Expanding secret patents to all dual-use technologies would severely infringe upon patent ownership rights, contradicting fundamental principles of patent law, property rights and international legal norms.

Furthermore, imposing strict secrecy provisions on dual-use technologies could lead countries to develop fragmented national patent systems, limiting technological exchange between jurisdictions. For instance, under a trade secrecy regime, competing firms might never learn about a rival's processes or incorporated technologies until a new product is publicly marketed (Kitch, 1977). This inefficiency results in wasted investments in rediscovering already-developed technologies.

A fragmented system could encourage countries to become more insular and less willing to share technological advancements in key sectors. While trade secrets may initially seem preferable to a secret patent system, they protect proprietary information. Trade secrets offer strategic advantages by safeguarding valuable information beyond patent expiration or preserving tacit knowledge that cannot be easily codified (Burk, 2016). In a world driven by patent disclosures, even if firms lack direct access to a competitor's technology, they can still learn from published patents and improve upon them. However, no such learning opportunity exists with trade secrets unless a competitor voluntarily discloses their advancements.

Therefore, a closed patent system is unsustainable in an era of increasing technological interconnectivity and global trade. While closed systems may protect proprietary technologies in the short term, they can impede long-term progress, especially in industries reliant on cross-border collaboration and shared knowledge. In conclusion, the absence of a viable compensation mechanism and the legal uncertainty surrounding inventors' rights make a broad secret patent system for dual-use technologies both legally and economically untenable.

3.2. Selective Disclosure of a Patent Application

Rather than completely removing dual-use inventions from the public domain and broadening the scope of secret patent regulations to all dual-use inventions, there is a middle-ground solution that can address

national technology security concerns and the need for open innovation. This involves keeping just part of a patent application secret, i.e. a dual-use invention's most valuable technical information, and is referred to as selective disclosure.

In this approach, there is no public disclosure of technical descriptions of a dual-use invention in a patent database, and access is limited to trusted parties only. In this context, selective disclosure means that the full technical details of a patent are only made accessible to certain authorised entities. In the context of dual-use technologies, this ensures that sensitive knowledge is protected from potential misuse, e.g. by hostile nations or non-state actors, while maintaining a system of legal recognition for the patent holder's exclusive rights.

Instead of complete secrecy, specific details could be redacted or made available only under particular conditions, governmental oversight or security clearances. These conditions may include the recipient's nationality, belonging to a list of trusted partners, entering into non-disclosure agreements or limiting access to specific industries. Rather than concealing the entire patent application, governments could classify technologies and provide tiered access depending on the sensitivity of the information. For example, some information could be made available to researchers or companies under specific licenses, while other sensitive aspects would be restricted.

The goal is to restrict public access to technological know-how while not conflicting with the patent owner's rights. As the proposal involves not disclosing some of the patent information, it does not prevent the inventor from commercialising their invention. Therefore, there is no need to develop a separate compensation system. The inventor is still free to commercialise the invention. While the technical description remains undisclosed, the patent still confers exclusive rights to the holder, allowing them to prevent others from making, using or selling the technology without authorisation.

A patent's legal enforceability would not change. However, if an infringement occurred, the detailed technical description would only be made available in a secure legal setting and possibly only to experts with an appropriate level of clearance. Courts overseeing infringement cases would require special clearance to access the technical description and only then in a closed environment. It must be emphasised that the patent holder should be able to file a petition to the patent office to have the non-disclosure order reviewed and possibly lifted.

The selective disclosure proposal could follow the example of measures in Article 5s of Regulation (EU) 833/2014. The EU and its member state IP offices flag a given IP right record held in their databases to indicate that the IP right has been frozen due to EU sanctions, while still allowing the frozen IP rights to be displayed in online databases. A parallel can be drawn with not disclosing the technical description of a dual-use technology patent application. The patent application (i.e. the technical description) should be redacted so that any sections concerning the technical description are blacked out or not displayed publicly, limiting access to this information to certain entities. The technical information should be flagged as sensitive due to its dual-use nature.

Instead of withholding the technical description, only those with appropriate clearance or certification would be allowed to view the full technical details of the patent. These trusted parties could include government agencies, relevant international organisations or specific entities with a proven need to know. For example, governments or relevant international organisations could have access to technical descriptions, while the broader public would only see minimal metadata. This means protocols must be developed to determine whether individuals qualify to be granted access. These protocols must be detailed, considering possible security risks. Conducting a thorough risk assessment of individuals seeking access rights should be mandatory.

Accordingly, a comparable identification mechanism has already been established within the EU legal framework, particularly in the context of EU sanctions concerning IP, as overseen by EUIPO. EUIPO and national IP offices in the EU are tasked with identifying the nationality and address of a patent applicant and verifying the names of owners or applicants of new patent applications, to decide whether

the applicant is eligible to apply for a patent. In addition to lists of names and other detailed procedures distributed to the EU national IP offices and other EU institutions, it has been noted that the European Commission, national IP offices and EUIPO may develop an IT solution to pre-check and pre-filter applications, so that applications filed by individuals who are sanctioned persons cannot enter the IT system (European Commission, 2024d).

A patent application for dual-use technologies must still be filed with the relevant patent office. The patent office would perform its usual formal examination procedures, including checking for novelty, inventive steps and industrial applicability. However, only basic metadata relating to the application would be published, instead of a full technical description, which typically includes diagrams, descriptions and claims. Selective disclosure should only be for a particular period, e.g. until technological security concerns subside. The latter must include the end of the Russia-Ukraine war. A similar practice was noted during World War II, when the United States issued more than 11,000 secrecy orders, of which the majority were rescinded at the war's end (Gross, 2019).

A question arises in the context of defining the boundaries of an invention and the practice of reinventing the same technology for the purpose of obtaining a new patent. To avoid unintentional infringement of someone else's IP, it is essential to identify all potentially restrictive patents and extract sufficient information to define the scope of exclusion (Devlin, 2010). One of the benefits of publishing patent applications is that it prevents duplicate efforts and avoids unnecessary costs. The information conveyed by patents serves a vital role in demarcating a patentee's IP interests. Although patent applications contain technical information, they may not always meet the level of detail required by a specialised technical community (Burk, 2016). In particular, the IT industry is known for producing patents that provide minimal, if any, insight into the true nature of the discovery (Devlin, 2010).

To prevent potential abuse of the selective disclosure system, patent offices could require a generic description or high-level overview to be published, which would not give away technical specifics but would provide sufficient information for competitors to understand the general scope of the invention. A high-level patent description would provide a general understanding of the invention, even if the specific technical methods, systems or mechanisms remain undisclosed. This would ensure that competitors understand the broad concept, reducing the likelihood of unintentionally duplicating the patent or infringing the patent owner's rights. A high-level overview should include a general description of the invention, its relevance to industry and the problem it solves. Specific technical details should be excluded as they are subject to non-disclosure.

Determining which dual-use technologies are eligible for selective disclosure regulations involves a careful process. The basis for identifying eligible dual-use items can be gleaned from the European Council's Common High Priority Items list. This ensures that not every technology is subject to selective disclosure restrictions, only those technologies that are considered high-priority.

As dual-use technologies can be applied for both civilian and military purposes, the task is to identify those technologies that require special handling due to their potential for misuse or their critical nature. This must involve expert review and risk assessments based on a technology's military potential, technological complexity and any relevant international security concerns. Some questions to address during the risk assessment could be how difficult it would be for an adversary to replicate or exploit the technology, whether the technology is unique and non-replicable, whether there are open-source or public alternatives, and how the technology might affect the strategic balance between international allies and adversaries.

It is important to emphasise that international collaboration on the protection of dual-use technologies is essential to ensure the efficiency of IP protection. As no universal patent database currently covers all patent documents published worldwide, such measures must be implemented internationally to secure the same approach for all Western countries. For instance, WIPO should coordinate international treaties or agreements to ensure that the selective disclosure system aligns with global security protocols. This coordination could involve setting standards for how such patents are dealt with internationally.

Furthermore, countries must coordinate on international frameworks or agreements to protect dual-use technologies without restricting them entirely and stifling innovation. Governments should collaborate with the private sector to establish frameworks via which companies can contribute to developing sensitive technologies while ensuring these inventions are protected from exploitation. Countries and organisations should be able to share information about dual-use patents within secure frameworks, such as those established in the NATO Agreement on the Communication of Technical Information for Defense Purposes.

In summary, selective disclosure protects sensitive technologies while allowing the patent holder to benefit from legal protection. Restricting access to specific parties ensures that dual-use technologies do not fall into the wrong hands, but it avoids the complete secrecy involved in a secret patent system. This maintains the incentive for innovation, as inventors still benefit from the exclusive rights granted by a patent without the risk of public exposure of their work. While selective disclosure offers advantages in safeguarding national security and preventing the misuse of sensitive technologies, the system must be carefully monitored to ensure it does not hinder the broader goals of innovation, knowledge sharing and global technological progress.

Conclusions

Sanctions have failed to fully restrict Russia's access to advanced technology due to its circumvention of sanctions and its use of illicit supply chains. A key vulnerability in the protection of IP rights is the public availability of technical details in patent databases, which adversaries can exploit.

I propose reforming the patent system by selectively disclosing only high-level descriptions for dual-use technology patents, keeping their technical details hidden. This would prevent the misuse of technological innovation while maintaining IP protection.

The selective disclosure approach balances technological security with open innovation, ensuring that only trusted entities have controlled access to critical technological information. Controlled access frameworks could allow vetted entities, such as trusted companies and allies, to view full technical details under non-disclosure rules. Periodic review would prevent indefinite secrecy.

Implementing selective disclosure internationally through bodies such as the World Trade Organization or WIPO would maximise the impact on protecting Western innovation. Regionally, EU legislation could enact these changes.

References:

United Nations. (1960, September 21). *Agreement for the mutual safeguarding of secrecy of inventions relating to defense and for which applications for patents have been made* (UN Treaty No. 5664). http://treaties.un.org/doc/Publication/UNTS/Volume%20394/volume-394-I-5664-English.pdf

World Trade Organization. (1994, April 15). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)*. Marrakesh Agreement Establishing the World Trade Organization, Annex 1C. https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

Anderson, J. J. (2011). Secret Inventions. *Berkeley Technology Law Journal, 26 917*, American University, WCL Research Paper No. 2011-33. https://ssrn.com/abstract=1970001.

Beckerman-Rodau, A. (2009). Patents Are Property: A Fundamental but Important Concept. *Journal of Business & Technology Law 4 (1)* https://digitalcommons.law.umaryland.edu/jbtl/vol4/iss1/4 accessed 4 March 2025.

Bergmann, M., et al. (2023). Out of Stock? Assessing the Impact of Sanctions on Russia's Defence Industry. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bergmann_Out_Stock.pdf?VersionId=6jfHCP0c13bbmh9bw4Yy2wbpjNnfeJi8 accessed 21 January 2025.

Bogers, M. (2012). Knowledge Sharing in Open Innovation: An overview of theoretical perspectives on collaborative innovation. open innovation in firms and public administrations: technologies for value creation, In C. de Pablos Heredero & D. López (Eds.), *Open Innovation in Firms and Public Administrations: Technologies for Value Creation* (pp. 1–14). IGI Global. https://doi.org/10.4018/978-1-61350-341-6.ch001

Burk, D. L. (2016). Patent Silences. *Vanderbilt Law Review*, 69(6), 1603-1630. https://escholarship.org/uc/item/0h78z072 accessed 22 January 2025.
Council of the European Union. (2024). *Council Decision (CFSP) 2024/1744 of 24 June 2024 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*. *Official Journal of the European Union, L 2024/1744*. http://data.europa.eu/eli/dec/2024/1744/oj
Council of the European Union. (2009). *Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast)*. *Official Journal of the European Union, L 134*, 1–269. http://data.europa.eu/eli/reg/2009/428/oj
Council of the European Union. (2014a). *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*. *Official Journal of the European Union, L 78*, 6–15. http://data.europa.eu/eli/reg/2014/269/oj
Council of the European Union. (2014b). *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*. *Official Journal of the European Union, L 229*, 1–11. http://data.europa.eu/eli/reg/2014/833/oj
Council of the European Union. (2022). *Council Regulation (EU) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. Official Journal of the European Union, L 49,* 1—140. http://data.europa.eu/eli/reg/2022/328/oj
Consolidated Versions Of The Treaty On European Union And The Treaty On The Functioning of The European Union. (2016). *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences. Official Journal of the European Union, C 202,* lk 1—388. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT
De Beer, J. (2021). Intellectual Property and 'open' innovation: A synthesis of concepts In I. Calboli & M. Rimmer (Eds.), *Handbook on intellectual property research*. Oxford University Press. https://doi.org/10.1093/oso/9780198826743.003.0046
Government of the Russian Federation. (2022, March 5). *Decree No. 430-p*. http://publication.pravo.gov.ru/Document/View/0001202203070001
Government of the Russian Federation. (2022, March 6). *Decree No. 299 on amending item 2 of the methodology of calculation of compensation's amount to be paid to patent owner resulting from decision to use invention, utility model or industrial design without patent owner's consent, and procedure of its payment*. http://publication.pravo.gov.ru/Document/View/0001202203070005
Devlin, A. (2010). The Misunderstood Function of Disclosure in Patent Law. *Harvard Journal of Law & Technology, Volume 23, Number 2.* https://jolt.law.harvard.edu/articles/pdf/v23/23HarvJLTech401.pdf accessed 1 February 2025.
Epifanova, A. (2023). *Tech sanctions against Russia: Turning the West's assumptions into lessons* (DGAP Analysis No. 3). German Council on Foreign Relations. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-87675-5 accessed 23 January 2025.
Estonian Parliament. (1994). *Patents Act (RT I 1994, 25, 406)*. https://www.riigiteataja.ee/en/eli/512072023002/consolide
European Commission general guidelines. (2023). List of economically critical goods. https://finance.ec.europa.eu/publications/list-economically-critical-goods_en accessed 21 December 2024.
European Commission general guidelines. (2024). List of common high priority items. https://finance.ec.europa.eu/publications/list-common-high-priority-items_en accessed 21 December 2024.
European Commission. (2023). State of play of EU-Türkiye political, economic and trade relations. https://neighbourhood-enlargement.ec.europa.eu/joint-communication-european-council-state-play-eu-turkiye-political-economic-and-trade-relations-0_en accessed 19 December 2024.
European Commission. (2024a). EU trade relations with Russia. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/russia_en accessed 23 January 2025.
European Commission. (2024b). EU and Partners Expand List of Common High Priority Items to Further Weaken Russia's War Effort. https://policy.trade.ec.europa.eu/news/eu-and-partners-expand-list-common-high-priority-items-further-weaken-russias-war-effort-2024-02-23_en accessed 20 December 2024.
European Commission. (2024c). EU adopts 14th package of sanctions against Russia for its continued illegal war against Ukraine, strengthening enforcement and anti-circumvention measures. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3423 accessed 30.12.2024.

European Commission. (2024d). Intellectual property rights. FAQs on sanctions against Russia and Belarus, with focus on the following legislation: Council Regulation (EU) No 269/2014; Article 5aa of Council Regulation (EU) 833/2014. https://finance.ec.europa.eu/publications/intellectual-property-rights_en accessed 19 January 2025.
European Commission. (n.d.). Sanctions on dual-use goods. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine/sanctions-dual-use-goods_en accessed 9 December 2024.
European Council. (2024). Russia's war of aggression against Ukraine: comprehensive EU's 14th package of sanctions cracks down on circumvention and adopts energy measures. https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/russia-s-war-of-aggression-against-ukraine-comprehensive-eu-s-14th-package-of-sanctions-cracks-down-on-circumvention-and-adopts-energy-measures/ accessed 30.12.2024.
European Council. (n.d.). EU sanctions against Russia explained. https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/ accessed 9 December 2024.
Feldstein, S.; Brauer, F. (2024). . Why Russia has been so resilient to Western export controls. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2024/03/why-russia-has-been-so-resilient-to-western-export-controls?lang=en
German Criminal Code (1998). Federal Law Gazette I, p. 3322. https://www.gesetze-im-internet.de/englisch_stgb/index.html
German Patent Act (1980). Federal Law Gazette 1981 I, p. 1. https://www.gesetze-im-internet.de/englisch_patg/englisch_patg.html
Giumelli, F. (2024). A comprehensive approach to sanctions effectiveness: Lessons learned from sanctions on Russia. *European Journal on Criminal Policy and Research, 30*(2), 211–228. https://doi.org/10.1007/s10610-024-09585-x.
Gross, D. P. (2019). The consequences of invention secrecy: Evidence from the USPTO patent secrecy program in World War II. *Harvard Business School Working Paper No. 19-090*. https://www.hbs.edu/faculty/Pages/item.aspx?num=55709 accessed 26.02.2025.
Herzog, S.; Dominika, K. (2024). NATO and emerging technologies—The alliance's shifting approach to military innovation. *Naval War College Review, 77*(2). https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/5 accessed 28 January 2025.
Interfax. (2024). (2024, January 16). *ФАС выступает за законодательное закрепление работы параллельного импорта на постоянной основе* [FAS advocates legislative consolidation of parallel import on a permanent basis]. *Interfax*. https://www.interfax.ru/business/968262
Janis, M.; Holbrook, T. (2012). Patent Law's Audience. *Minnesota Law Review, 97,* 72-123. https://www.repository.law.indiana.edu/facpub/788/
Kitch, E. W. (1977). The Nature and Function of the Patent System. *The Journal of Law and Economics*, 20(2), 265-290 https://doi.org/10.1086/466903
Kolyandr, A. (2024). Tightening the Screw? — EU's New Sanctions on Russia. *Center for European Policy Analysis (CEPA)*.https://cepa.org/article/tightening-the-screw-eus-new-sanctions-on-russia/
Latvian Patent Law (2007). Latvijas Vēstnesis, 34, 27.02.2007. https://likumi.lv/ta/en/en/id/153574-patent-law
Leminen, S., Westerlund, M., Rajahonka, M., & Siuruainen, R. (2015). The grey areas between open and closed in innovation networks. *Technology Innovation Management Review, 5*(12), 6–18.http://doi.org/10.22215/timreview/948
Lithuanian Patent Law (1994). Official Gazette No 8-120, 1994, ID code 0941010ISTA000I-372. https://vpb.lrv.lt/uploads/vpb/documents/files/Patent%20Law.pdf
Marcus, J. S., et al. (2022, March 28). The decoupling of Russia: High-tech goods and components. *Bruegel*. https://www.bruegel.org/blog-post/decoupling-russia-high-tech-goods-and-components
Mosolova, D.; Fleming, S. (2023). West Probes Potential Sanction Dodging as Exports to Russia's Neighbours Surge. *Financial Times*, 23 February 2023. https://www.ft.com/content/4961a96c-16ac-496b-8aba-16d6025e4dfe
Murilo Rangel Da, S. (2025). Western Sanctions against Russia in the Ukraine War: Effects of Russian Strategies on the Development of Multilateralism. *Open Journal of Social Sciences*, *13*(1), 400–418. https://doi.org/10.4236/jss.2025.131025
United States Department of State. (1970, October 19). *NATO Agreement on the Communication of Technical Information for Defense Purposes*. https://www.state.gov/nato-technical-information-for-defense-purposes
OECD. (2008). Competition, Patents and Innovation. https://www.oecd.org/en/publications/competition-patents-and-innovation_3d4b7785-en.html accessed 02.02.2025.
OECD. (2018). Oslo Manual 2018. https://www.oecd.org/en/publications/oslo-manual-2018_9789264304604-en.html accessed 03.02.2025.
Orlov, A. (2024, September 4). Inside Russia's 2024 military-industrial complex. *European Security & Defence*. https://euro-sd.com/2024/09/articles/40149/inside-russias-2024-military-industrial-complex/

Põld, L. (2024). Preserving Secrecy within the Patent System to Safeguard Western Countries' Technological Innovation. *Juridica International, 33*, 77–88. https://doi.org/10.12697/JI.2024.33.06
Ponchek, T. (2016). The Emergence of The Innovative Entity: Is The Patent System Left Behind? UIC Review of Intellectual Property Law, Vol 16, Iss 1. https://repository.law.uic.edu/ripl/vol16/iss1/4/ accessed 02.02.2025.
Rantanen, J. (2013). Patent law's disclosure requirement. *Loyola University Chicago Law Journal, 45*(2) https://lawecommons.luc.edu/luclj/vol45/iss2/3 accessed 22 January 2025.
Renda, K. K., Kaya, A., & Yesil, S. (2023). Turkey's proactive contestation of EU sanctions against Russia: European normative order vs. geopolitical realities. *Southeast European and Black Sea Studies, 23*(4), 757–780. https://doi.org/10.1080/14683857.2023.2273021
Rooke, J. (2024, May 22). Special report: Unveiling Western business implications in the Russian defence industry's supply chains. *NATO Association of Canada (NAOC)*. https://natoassociation.ca/unveiling-western-business-implications-in-the-russian-defence-industrys-supply-chains/
Scazzieri, L. (2024). The EU and Türkiye: A relationship adrift. *Centre for European Reform*.. https://www.cer.eu/insights/eu-and-turkiye-relationship-adrift
Seymore, S. B. (2010). The teaching function of patents. *Notre Dame Law Review, 85*(2), 621–669.https://ssrn.com/abstract=1352044
Shagina, M. (2023, November 9). Why can't the West stop supplying technology for Russian weapons? *Foreign Policy* https://foreignpolicy.com/2023/11/09/russia-sanctions-weapons-technology-exports-evasion-arms-production-missiles-chips/
Sherman, J. (2024, July 29). Russia's digital tech isolationism: Domestic innovation, digital fragmentation, and the Kremlin's push to replace Western digital technology. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-digital-tech-isolationism/
Swanson, A., & Chokshi, N. (2023, May 15). U.S.-made technology is flowing to Russian airlines, despite sanctions. *The New York Times*. https://www.nytimes.com/2023/05/15/business/economy/russia-airlines-sanctions-ukraine.html
Trade with Estonia. (2025). Estonian technology company Nortal signs agreement with NATO. *Trade with Estonia*. https://tradewithestonia.com/estonian-technology-company-nortal-signs-agreement-with-nato/
Petrova, V., & Sapozhkov, O. (2023, April 10). A thought limited by flight altitude (Мысль с ограничением по высоте полета). *Kommersantъ*. https://www.kommersant.ru/doc/5925857
Ministry of Industry and Trade of the Russian Federation. (2022, April 19). *Order No. 1532 "On the approval of the list of goods (groups of goods) to which the provisions of subparagraph 6 of Article 1359 and Article 1487 of the Civil Code of the Russian Federation do not apply, provided that such goods are introduced into circulation outside the territory of the Russian Federation by right holders (patent holders), or with their consent"* (Приказ Минпромторга РФ № 1532 от 19.04.2022 г.). https://base.garant.ru/404580514/