CITP
CENTRE FOR INCLUSIVE TRADE POLICY

@centre4itp

National security and intellectual property protection of critical technologies

Phoebe Li and Atilla Kasap

Published 2 October 2025

Briefing Paper 26

Key Points

- National industrial strategies for building critical technologies challenge the scope of 'national security' in international intellectual property protection.
- National security provisions in the World Trade Organization (WTO) are traditionally considered narrowly in the military context or 'an emergency in international relations' where actions are necessary to safeguard countries' essential security interests. However, they do not address the issues around cybersecurity.
- Many recent preferential trade agreements have expanded the scope of national security to include cybersecurity-related measures.
- Despite the US's withdrawal from the multilateral trade system, it is still desirable to harmonise the interpretation of national security in the international investment and intellectual property context.
- A broader scope of national security should encompass cybersecurity and a multistakeholder model for governing critical technologies in order to ensure inclusivity and participation of civil society.

Introduction

Intellectual property (IP) protection, particularly patenting, has been a key driver for innovation as it provides legal frameworks for protecting inventors' and investors' rights and ownership on innovative information and know-how. It offers limited periods of market monopoly for IP owners to exercise their control and decide how the knowledge could be used in society. However, this right is often constrained by other legitimate interests such as competition, consumer welfare, and national security issues, which are typically called 'exceptions' to IP. In recent years, innovations in critical technologies combined with national security issues have blurred the IP landscape. This is evident with the US-China trade war in which national security claims are centred on economic security and related IP issues.

This Briefing Paper maps the evolving IP ecosystem due to the expansion of national security claims and innovation in critical technologies, drawing examples from protecting information on AI, semiconductor chips, and quantum computing. The Briefing Paper also makes recommendations for how to improve the balance of concerns between IP protection and national security going forward.

What are critical technologies?

The meaning and the scope of what constitutes 'critical technologies' varies across countries. A technology deemed critical in one country may not be considered as such in another. The differentiation of technologies is based on the country's public interests, industrial policy and national security. For example, the US Directorate for Technology, Innovation and Partnerships (TIP) focused on accelerating work in selected critical technology areas, such as advanced manufacturing, advanced materials, advanced wireless, artificial intelligence, biotechnology, quantum information science and semiconductors and microelectronics.[1] The European Commission has identified advanced semiconductors, AI, quantum technologies, and biotechnologies, as four critical technologies that are highly likely to pose the most immediate, sensitive risks with regards to technology security and leakage.[2] Similarly, the UK has been navigating the new regulatory approaches for digital economy by setting out the UK Digital Strategy in 2021. It identified the UK's leadership in artificial intelligence, advance semiconductor design and quantum computing.[3] The National Science and Technology Council (NSTC) also identified three sectors as priority areas - AI,[4] semiconductors,[5] and quantum technologies.[6] In sectors where the key industry depends on the import of vital goods, the UK Department for Business & Trade highlighted advanced manufacturing, semiconductors, batteries and critical minerals as priority sectors for securing supply chain resilience.[7] Overall, artificial intelligence, semiconductors, quantum computing, and critical minerals are deemed as priority sectors in the UK industrial strategies.

National security in the WTO

There are national security provisions under the General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS), and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). These allow for exceptions to the general rules on specified grounds of national security. Article XXI of the GATT, emphasises 'essential security interests,' which allows Parties to:

i) Withhold any information they consider harmful to these interests if disclosed;

ii) Take any actions deemed necessary for: a) managing fissionable materials; b) controlling the trafficking in arms, ammunition, and war implements, or any other trade in goods and materials intended for military supply; c) acting during times of war or other international emergencies;

iii) Fulfill their obligations under the United Nations Charter for maintaining international peace and security. This provision grants Parties some latitude to invoke the national security defence, as it allows them to use their discretion in deciding which actions are necessary to safeguard their essential security interests.[8] As a result, its application has been 'broad, self-defining, and ambiguous'.[9]

The invocation of Article XXI to justify protectionist trade measures across the world has undergone some, though limited, scrutiny by the WTO. We briefly review the cases below.

The first WTO panel report involving Article XXI was *Russia - Measures Concerning Traffic in Transit* (WT/DS512), issued in 2019.[10] Ukraine complained about Russia's restrictions on the transit of Ukrainian goods through Russia's territory. Russia claimed the trade restrictions were adopted in the context of 'an emergency in

---

[1] U.S. National Science Foundation, 'Technology: Paving the Way for the Technologies That Will Shape the Future', https://new.nsf.gov/focus-areas/technology accessed 4 July 2025.

[2] Commission, 'Commission Recommendation of 3.10.2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States' C (2023) 6689 final, 2.

[3] Department for Digital, Culture, Media & Sport, 'UK Digital Strategy' (4 October 2022), 4 https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy accessed 3 July 2025.

[4] HM Government, *National AI strategy* (Cmd 525, 2021) 4. Note the NSTC was set up to advise the previous government and has now been converted into a Cabinet Committee.

[5] Department for Digital, Culture, Media & Sport, 'Government Explores National Initiatives to Boost the British Semiconductor Industry' (5 December 2022) https://www.gov.uk/government/news/government-explores-national-initiatives-to-boost-the-british-semiconductor-industry
accessed 4 July 2025.

[6] Department of Business, Energy & Industrial Strategy, 'UK Quantum Strategy: Call for Evidence' (2022) https://assets.publishing.service.gov.uk/media/620a86d2d3bf7f4f0276071e/uk-quantum-strategy-call-for-evidence.pdf accessed 4 February 2024; Department for Science, Innovation & Technology, 'Science & Technology Framework: Taking A Systems Approach to UK Science & Technology' (2023), 5 https://assets.publishing.service.gov.uk/media/6405955ed3bf7f25f5948f99/uk-science-technology-framework.pdf accessed 4 July 2025.

[7] Department for Business & Trade, 'Critical Imports and Supply Chains Strategy', 17 January 2024, https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy/critical-imports-and-supply-chains-strategy-html-version, accessed 4 July 2025.

[8] Tatiana Lacerda Prazeres, 'Trade and National Security: Rising Risks for the WTO' (2020) 19(1) WTR 137, 138.

[9] John H. Jackson, *The World Trading System* (2nd edn, MIT Press 1997) 230.

[10] Panel Report, *Russia – Measures Concerning Traffic in Transit* (*Russia-Traffic in Transit*), WT/DS512/R.

international relations'. The Panel held that the test for reviewing the measure involved subjective and objective steps. While the adjective clause 'which it considers necessary' provides leeway for WTO Members to define their essential security interests on good faith, there are overall objective assessments on what constitutes 'emergency' in international relations. There was discretion on the Member invoking Article XXI, but it was subject to the WTO review. Here, the Panel accepted Russia's arguments and concluded that an emergency in international relations generally referred to a situation of armed conflict, heightened tensions or crisis, or general instability surrounding a state.

Another dispute in which the national security defence was invoked is *United States–Certain Measures on Steel and Aluminium* (WT/DS552), decided in 2022. Following the imposition of certain measures (tariffs) and duties (product-specific exclusions) on steel and aluminium imports by the US, a number of countries brought disputes against the US at the WTO.[11] The WTO panel held that an 'emergency in international relations' amounts to a situation of particular gravity or severity, and international tensions that are of a critical or serious nature regarding their impact on the conduct of international relations.[12] Based on these conditions, the WTO panel rejected the US's argument and concluded that the factors affecting the US's trade measures did not fall within the scope of an 'emergency in international relations'.[13]

In determining the scope for invoking the national security exception in the TRIPS Agreement, in 2020, the Panel in *Saudi–Protection of IPR* (WT/DS567/R) stated that the severance of diplomatic relations does not necessarily result in the non-application of the multiple agreements on trade in goods, the GATS, or the TRIPS Agreement (para. 7.22).[14] The recent dispute concerning national security, *the United States – Origin Marking Requirement*, stemmed from the US policy of labelling imported goods made in Hong Kong as originating from China.[15] The Panel defined 'an emergency in international relations' as an extremely serious situation involving states or other entities, which can result in or approach a total collapse of relations. [16] The Panel further clarified that such an emergency does not have to be linked to military or defence-related issues. [17]

In sum, there is some discretion for the Member invoking the 'national security' exception, but the invocation is subject to WTO review. The test for reviewing the measure involves both subjective and objective steps, and the objective steps generally apply to narrow interpretations of armed conflicts, heightened tensions or crisis, or general instability surrounding a state.

Cybersecurity and international public policy

Recently, particularly following the Russia-Ukraine war, cyberattacks by state actors and ransomware demands against public and private institutions in the Western world have noticeably surged. However, GATT/GATS law is not keeping pace, with no clear understanding of how to include cybersecurity within the scope of national security. While the interpretation of 'national security' under Article XXI of GATT is self-defining, broad and ambiguous, it has historically been understood in a narrow context that does not explicitly incorporate cybersecurity concerns.[18] This creates a gap, which has become more evident as cyber threats increasingly threaten both economic and national security,[19] and specifically targeted the theft of IP.[20] The article's scope was not drafted with cybersecurity in mind, and as such, there is a pressing need for an updated interpretation that accounts for this emerging threat.

---

[11] These disputes were initiated by China (WT/DS544), India (WT/DS547), the European Union (EU) (WT/DS548), Norway (WT/DS552), Russia (WT/DS554), Switzerland (WT/556), and Turkey (WT/DS564) against the United States. Mexico (WT/DS551) and Canada (WT/DS550) also opened cases, but mutually agreed solutions with the United States were later announced.

[12] Panel Report, *United States–Certain Measures on Steel and Aluminium Products*, WT/DS552/R, para. 7.127.

[13] Para. 7.131.

[14] Panel Report, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, WT/DS567/R (adopted 16 June 2020).

[15] Panel Report, *United States – Origin Marking Requirement*, WT/DS597/R (adopted 21 December 2022).

[16] Para. 7.290.

[17] Para. 7.301.

[18] Gregory Shaffer, 'Trade Law in a Data-driven Economy: The Need for Modesty and Resilience' (2021) 20(3) WTR 259, 275.

[19] See, e.g., International Monetary Fund, 'Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks' (2024), 77 https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024 accessed 4 July 2025 (reporting that the number of cyberattacks has approximately doubled since the COVID-19 pandemic).

[20] Debora Halbert, 'Intellectual Property Theft and National Security: Agendas and Assumptions', (2016) 32 Info Soc'y 256, 268.

Many recent preferential trade agreements (PTAs), including Digital Economy Partnership Agreement (DEPA), Regional Comprehensive Economic Partnership (RECP), Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and United States-Mexico-Canada Agreement (USMCA), have already expanded the scope and flexibilities of national security to include cybersecurity-related measures.[21] This highlights the increased awareness of the importance of these issues, but which have not yet been translated into WTO provisions. The WTO Joint Statement Initiative (JSI) on e-commerce began with 71 members exploring future WTO negotiations on trade-related aspects of e-commerce and has grown to 91 members as of 25 June 2024. The JSI reached a stabilised text on 26 July 2024. The proposed general and security exceptions in the WTO e-commerce stabilised text reaffirm the continuity of the exception provisions[22] under GATT/GATS, without addressing any cybersecurity vulnerabilities.[23]

The approach adopted in the stabilised text is different from the explicit inclusion of separate cybersecurity provisions in some PTAs which, for example, oblige Parties to implement cybersecurity incident response measures and collaborate against malicious attacks (for example, Article 19.15 of USMCA). Despite acknowledging the significant threat cybersecurity poses to e-commerce, the final proposed WTO text does not provide sufficient legal flexibility for countries to take measures in response to cyber threats, thereby preserving the legal lacuna that exists in Article XXI of GATT. The final text does not provide legal grounds for countries to take measures.

This is not because of a lack of awareness of the issue. Indeed, an earlier formulation in the negotiations, within the general exception provisions allowed parties to take measures to protect cybersecurity, cyberspace sovereignty, the legal rights and interests of its citizens, legal persons, and other organisations, and to achieve other lawful public policy objectives.[24] However, this formulation has not been adopted in the stabilised text, though participants have left the door open for potential inclusion in future negotiations. The need to broaden the scope of general exceptions under GATT/GATS remains.

With the US effectively pulling out of the multilateral rule book, the WTO should proceed in a plurilateral fashion without the US and build minimum standards on national security reflected in recent trade agreements, such as the CPTPP and USMCA, with a view to harmonising the scope of national security in intellectual property. At first, the US was a leading proponent of digital trade rules, but later it withdrew its support for several proposals. It appears that the absence of the US during negotiations helped participants reach consensus on the JSI's stabilised text by lowering ambition on sensitive digital trade issues—particularly cross-border data flows and the scope of exceptions. Finally, the US considered the WTO's stabilised text to be an important step forward, but also believed it still required more work, especially regarding the essential security exception.[25]

WTO law has often historically evolved through the absorption and refinement of optimal norms initially developed within PTAs, which often serve as laboratories for regulatory innovation and experimentation in international trade. For example, the broad framing of security exceptions in recent PTAs, which omit specific conditions for invoking such exceptions, reflects a shift that potentially addresses emerging issues like cybersecurity.[26]

Foreign direct investment, critical technologies and national security

[21] Neha Mishra, *International Trade Law and Global Data Governance: Aligning Perspectives and Practices* (Hart, 2024) 86.
[22] Exception provisions found in WTO agreements permit member countries to adopt violating measures on the grounds of achieving public policy objectives, such as public health.
[23] WTO, *Joint Statement Initiative on Electronic Commerce*, INF/ECOM/87, 26 July 2024. (Articles 22 & 23 of the Agreement on Electronic Commerce).
[24] WTO, *WTO Electronic Commerce Negotiations Consolidated Negotiating Text - December 2020* INF/ECOM/62/Rev.1 (Annex I, section (6)), https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf accessed 4 July 2025.
[25] Statement by Ambassador María L. Pagán on the WTO E-Commerce Joint Statement Initiative, (July 26, 2024), https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative/ accessed 10 September 2025.
[26] Shin-yi Peng, 'Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions', (2023) 117 AJIL Unbound 122, 126.

National security concerns have also played a significant role in foreign direct investment (FDI) involving critical technologies, which are in turn closely linked, though not always, to intellectual property concerns. Notably, the recent America First Investment Policy explicitly expresses that economic security is national security and identifies that 'PRC[China]-affiliated investors are targeting the crown jewels of United States: technology, food supplies, farmland, minerals, natural resources, ports, and shipping terminals'.[27] However, restricting FDI due to national security reasons may lead to investor uncertainty and increase the risk of politicisation. The UK National Security and Investment Act (NSIA) took effect in 2022 and grants the government power to screen foreign direct investment in relation to transactions of sensitive sectors that may pose national security risks.[28] The absence of a clear definition for 'national security' under the NSIA inherently results in the broad application of the legislation. For instance, would increasing competition in the domestic market be sufficient grounds to restrict FDI involving 'ideas, information, or techniques that have industrial, commercial, or other economic value' under the NSIA?[29]

Some commentators have argued that in practice, the implementation of the NSIA has become excessively broad and lacks transparency for industry stakeholders. Some businesses[30] and legal practitioners[31] have expressed concern that the scope of transactions subject to review has expanded significantly, and that the criteria for triggering reviews are not always clear, leading to uncertainty. Between 1 April 2023 and 31 March 2024, the UK Government received 906 notifications—an increase from 865 in the previous year.[32] Although the overwhelming majority of notifications did not require further action, a considerable number (37) were scrutinised by the UK Government. More importantly, the percentage of critical technologies targeted under the NSIA is notable. These include data infrastructure, advanced materials, artificial intelligence, computing hardware, and advanced robotics. During the COVID-19 pandemic, when the semiconductor supply chain was disrupted, many acquisitions involving this technology were blocked. Unsurprisingly, these technologies have also seen a dramatic increase in patenting activity worldwide.[33]

Specifically, two recent examples showcased the UK's desire to protect critical infrastructure and intellectual property. The first being the acquisition of the shares in the biggest telecommunication company (BT), which was scrutinised by the UK Government in 2022 because telecommunication was deemed part of the UK's critical national infrastructure.[34] Although the UK Government ultimately decided not to take further action, this instance demonstrated the uncertainty around the application of the criteria. Additionally, the lack of a clear timeline for the screening process leaves the transacting parties navigating a highly unpredictable regulatory environment. Aware of these deficiencies in the NSIA (and its practical application), the UK Government has begun consultations on potential legal amendments that will create a more predictable, proportionate, and transparent screening framework as part of its 2025 Industrial Strategy.[35]

---

[27] The White House, 'America Frist Investment Policy' 21 February 2025, https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/ accessed 4 July 2025.

[28] National Security and Investment Act 2021 (NSIA 2021) s1(1).

[29] § 7(4)(c).

[30] See, e.g., Ashley Armstrong and Jim Pickard, 'UK Takeover Scrutiny to be Relaxed as Part of Industrial Strategy', (*Financial Times* 24 June 2025), https://www.ft.com/content/059b4bb1-0258-4536-9bbe-e2353c511772 accessed 24 June 2025 (reporting companies' criticisms against the implementation of the NSIA as opaque and excessively broad).

[31] Robert Gardener et. al., 'The National Security and Investment Act 2021: A Review of the Regime's First Year in Operation', (13 January 2023) https://www.hoganlovells.com/en/publications/the-national-security-and-investment-act-2021-a-review-of-the-regimes-first-year-in-operation (stating that the NSIA is 'unsurprisingly complex' and more opaque than other legal processes) accessed 4 July 2025.

[32] Cabinet Office, 'Corporate Report: National Security and Investment Act 2021: Annual Report 2023-24 (HTML)' (7 October 2024) https://www.gov.uk/government/publications/national-security-and-investment-act-2021-annual-report-2023-24/national-security-and-investment-act-2021-annual-report-2023-24-html.

[33] See, e.g., European Patent Office, 'Patents and the Fourth Industrial Revolution' (December 2020), 29, https://link.epo.org/web/patents_and_the_fourth_industrial_revolution_study_2020_en.pdf .

[34] Department for Business, Energy & Industrial Strategy, 'Government to Take No Further Action under National Security and Investment on BT Share Acquisition' (23 August 2022) https://www.gov.uk/government/news/government-to-take-no-further-action-under-national-security-and-investment-act-on-bt-share-acquisition#:~:text=The%20government%20has%20decided%20to,shares%20by%20Altice%20in%20BT.&text=The%20acquisition%20by%20Altice%20of,Kwarteng%20on%20Thursday%2026%20May accessed 4 July 2025.

[35] Department for Business and Trade, 'The UK's Modern Industrial Strategy' CP1337 (June 2025), 45, https://assets.publishing.service.gov.uk/media/68595e56db8e139f95652dc6/industrial_strategy_policy_paper.pdf

The second example involved a potential FDI in semiconductor technology. In the same year of the BT screening (2022), the Department for Business, Energy and Industrial Strategy (BEIS) made an order of divestment in relation to a Chinese acquisition of a semiconductor wafer factory. After the security review, the government considered it a risk to national security due to the leak of 'technological expertise and know-how' to China.[36] During the decision-making process, the transacting party complained that the UK Government neglected their offers of extensive remedies to mitigate national security risks.

The blocked sale of a UK semiconductor company to a Chinese entity also highlighted a potential clash between the China-UK Investment Agreement, as international law, and the NSIA, as domestic law. Here a delicate balance needs to be struck between national security and fair and equitable treatment, as the China–UK Investment Agreement requires fair and equitable treatment to Chinese investments.[37] If such treatment is not provided, disputes between the UK and China under the agreement should, where possible, be resolved through diplomatic channels; if that fails, they are to be submitted to a binding arbitral tribunal constituted in accordance with Article 8 of the agreement. This agreement lacks an exception clause, thereby restricting a state's ability to implement measures based on national security concerns.[38] However, Article 2(1) of the UK-China Agreement states that each Party's commitment to promote and safeguard investment is constrained by the authority provided under its own domestic laws, including the UK's national security laws like the NSIA. If China chooses to initiate proceedings, an arbitral tribunal could assess whether the UK's action breached the terms of the agreement.

Intellectual property in critical technologies and national security: the conflicting needs for transparency and secrecy

The protection of intellectual property in critical technologies involves different layers of consideration of national security, as arguments could be made in both ways. In some scenarios, retaining secrecy (i.e., protection of IP) is essential for security, especially when it relates to cybersecurity, where digital and physical safeguards would be critical to combat cyberattack. In others, disclosure of information is required where such disclosure is essential for meeting the basic principles of algorithmic governance, including the principles of fairness, accountability, transparency, privacy, safety and security.

Article 27 of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) obligates Members to make all fields of technology patentable, yet recent innovation in critical technologies has shifted towards the protection of trade secrets as opposed to patenting, due to the higher requirements of disclosure for patentability. Patents are registered intellectual property rights granted for inventions that are novel, involve an inventive step, and are industrially applicable. Trade secrets, on the other hand, are commercially valuable information kept confidential by the holder and do not require registration to receive legal protection. For example, in cases where quantum computing incorporates AI—forming QC/AI hybrids leveraging the strengths of both technologies—the requirement for patent disclosure continuously raises the bar of patentability for follow-on applications, as in the case of requiring the disclosure of additional training data. Therefore, trade secrets are an easier route for protecting quantum technologies as it is difficult to reverse engineer, coupled with the fact that it is likely to be physically located, which makes it easier to keep it secret.[39] In recent international trade agreements, we can see that the rise in the ban of source code disclosure where trade secrets protection is claimed to protect software and algorithms; however, this claim would significantly conflict with the transparency requirement in digital data governance. However, further discussion of digital data governance is outside the scope of this Briefing Paper.[40]

[36] Department for Business, Energy & Industrial Strategy, 'National Security and Investment Act 2021: Publication of Notice of Final Order' (16 November 2022) https://www.gov.uk/government/publications/acquisition-of-newport-wafer-fab-by-nexperia-bv-notice-of-final-order accessed 4 July 2025.

[37] Agreement between the United Kingdom of Great Britain and Northern Ireland and China concerning the Promotion and Reciprocal Protection of Investments (adopted 15 May 1986, entered into force 15 May 1986) 1986 UNTS 101 (Article 2).

[38] Pascale Accaoui Lorfing, 'Screening of Foreign Direct Investment and the States' Security Interests in Light of the OECD, UNCTAD and Other International Guidelines' in Catharine Titi (ed), *European Yearbook of International Economic Law: Public Actors in International Investment Law* (Springer 2021), 195.

[39] Mateo Aboy, Timo Minssen and Mauritz Kop, 'Mapping the Patent Landscape of Quantum Technologies: Patenting Trends, Innovation and Policy Implications' (2022) 53 IIC 853, 869.

[40] See CITP & UKTPO Written Evidence to the International Agreements Committee, 18 October 2024, https://committees.parliament.uk/writtenevidence/131055/pdf/ for a discussion of these issues.

Recommendations for national security and the regulatory space in IP

In order to appropriately deal with the balance between national security and intellectual property in the age of digital development, we propose an expansive interpretation of 'national security' in TRIPS Article 73. This interpretation should explicitly include 'cybersecurity' and be aligned with the objectives and principles outlined in Articles 7 and 8 of TRIPS, which aim at ensuring a fair balance of stakeholders' rights and obligations, and promoting the public interest in sectors crucial to socio-economic and technological development.

In addition to including cyber-security as part of the working interpretation of national security, we also argue for the establishment of 'conditional rights' as a working framework. This would allow countries to implement trade measures based on national security concerns, provided that certain conditions are met. Conditional rights enjoy a higher-level status than ordinary exceptions since it is considered as a right instead of a defence.[41] Conditional rights are not exceptions to general rules but have a self-standing status that carves out the general rules in a mutually exclusive manner.[42] In other words, it is not being 'excepted' from, it is being replaced by another normative framework. Conditional rights imply an 'autonomous' basis for action that displaces the rule entirely, in applicable situations. They are autonomous rights, which means states have the discretion in claiming or invoking the right. The invocation of such a right would be deemed legitimate by default. Hence, the burden of proof is on the complaining party to prove that national security does not exist in the specific context. If this were just an exception, the burden would typically fall on the invoking party to justify why the general rule should not apply.

As an example of a conditional right, governments have the right to issue a compulsory licence under Article 31 of the TRIPS to permit a third party to manufacture a patented invention without the consent of the patent holder. The conditions for successfully invoking such licences include, among others: situations such as a national emergency; other circumstances of extreme urgency; or public non-commercial use; the requirement that the use be non-exclusive and non-assignable; and that it be predominantly for the supply of the domestic market. In the context of pharmaceutical products, the aim is to produce affordable generics or import them from third countries. For developing or less-developed countries that lack manufacturing capabilities, Article 31(bis) introduces important exemptions, such as allowing for the bypass of the requirement to predominantly supply the domestic market under certain conditions. The compulsory licensing mechanism under Article 31(bis) of TRIPS has been used between Rwanda and Canada in 2007 for importing HIV/AIDS drugs.[43] During the COVID-19 pandemic, several countries amended their national laws to facilitate the expedited issuance of compulsory licences in order to ensure access to affordable vaccines.[44] However, the scope of Article 31(bis) is limited to pharmaceutical products in order to facilitate access to medicine in developing and less-developed countries. The language of Article 31 is limited to extreme emergency situations, which may not encompass all cybersecurity-related emergencies in the digital sphere. As an interesting proposal, the International Association for the Protection of Intellectual Property suggested that it is unnecessary to distinguish between different technical fields when defining overriding interests where public interests are at stake.[45] We support this proposal and argue that compulsory licences, as conditional rights, should be invoked in response to cybersecurity incidents that may have a detrimental impact on the public interest.

Notably, the WTO Panel in *US – Origin Marking Requirement* understood 'an emergency in international relations' to mean a highly serious situation involving states or other actors, typically resulting in or approaching a total collapse of diplomatic relations.[46] Concerning situations of the highest seriousness, the Panel clarified that an emergency does not have to pertain to military or defence issues.[47] Given the Panel's broad

[41] Phoebe Li, *Health Technologies and International Intellectual property: A Precautionary Approach* (Routledge 2014).
[42] Steve Charnovitz, Lorand Bartels, Robert Howse, Jane Bradley, Joost Pauwelyn and Donald Regan, 'The Appellate Body's GSP Decision' (2004) 3(2) WTR 239, 257.
[43] WTO, 'Canada is First to Notify Compulsory Licence to Export Generic Drug' https://www.wto.org/english/news_e/news07_e/trips_health_notif_oct07_e.htm accessed 4 July 2025.
[44] See, e.g., Part 12 of An Act Respecting Certain Measures in Response to COVID-19, S.C. 2020, C-13 (Canada).
[45] AIPPI, Q293-RES-P-2025, (16 September 2025), https://aippi.soutron.net/Portal/Default/en-GB/DownloadImageFile.ashx?objectId=10162&ownerType=0&ownerId=6325 accessed 29 September 2025.
[46] Panel Report, *United States – Origin Marking Requirement*, WT/DS597/R (adopted 21 December 2022), para. 7.290.
[47] Para. 7.301.

interpretation, pandemics could also be considered emergencies in international relations.[48] Other conditions could include ensuring resilient supply chains, preventing dangerous military use, and targeting economic security. Moreover, a two-stage good faith test could be used to prevent abuse of the security exception clause, focusing on the reasonableness of classifying cybersecurity as an essential security interest and the genuine necessity of protective measures.[49]

However, the caveat lies in the risk of the abuse of such broad provisions. The growing invocation of Article XXI in recent trade disputes risks enabling protectionist abuse, undermining WTO multilateralism, eroding legal certainty, and setting a dangerous precedent that could extend to IP and TRIPS exceptions.[50] In order to prevent such abuse, we propose (below) the inclusion of multi-stakeholder participation for balancing the subjective and objective tests when invoking security exceptions.

Based on this minimum threshold for invoking the conditional right, we suggest that multi-stakeholders should be included in the decision-making process to determine whether the threshold is met. Multi-stakeholder engagement would focus on regulatory cooperation and collaboration on cybersecurity issues and engagement with broader stakeholders, including industrial experts as technical expert committees, institutional mechanisms and technical standards as evidence when assessing whether the conditionality was met.[51] Multi-stakeholder engagement would apply both before and after invoking the (conditional) national security restriction. Initially, before invocation, the invoking country should engage in multi-stakeholder consultation. If a dispute is raised after the invocation, the WTO review of the use of conditionality should also be conducted with multi-stakeholders involvement. Since government decisions on national security inherently involve confidential information, full disclosure to multi-stakeholders during such evaluations is not realistic. Nevertheless, governments must at least persuade relevant stakeholders that global cybersecurity norms and international standards have been violated. Disclosure could be contained in a predefined group of experts.

Furthermore, involving civil society in multi-stakeholder engagement would introduce innovative perspectives on the issue. This is especially crucial as emerging technologies such as AI are becoming increasingly prevalent in society and present distinct challenges—ranging from societal risks like disinformation to economic concerns such as unemployment, and environmental impacts like higher energy consumption. As a potentially highly-impacted stakeholder, civil society should actively participate in the decision-making process, for example, if AI-based technology imports from third countries are restricted or if FDI in critical technologies with the potential to boost employment is blocked on national security grounds.

Conclusion

Intellectual property protection of critical technologies requires a delicate balance between national security, competition and innovation. In general, recent FTAs have already reflected scope for accommodating cybersecurity, states may directly use this flexibility and do not need to trigger the contentious 'national security' clause, as is the case in the WTO. In this Briefing Paper, we propose to broaden the scope of 'national security' in the WTO TRIPS Agreement in order to accommodate the surging needs for cybersecurity in recent decades. We also advocate that 'national security' should be a conditional right instead of being an exception to WTO principles. In order to avoid abuse, we further suggest a multistakeholder approach as a conditionality for invoking national security grounds, by engaging a wide range of stakeholders, technical expert committees, industrial standards and civil society. In doing so, the inclusive approach to IP could contribute to the balance of

[48] Emmanuel Kolawole Oke, 'War, Armed Conflict, and the Security Exception in the TRIPS Agreement' (2024) 3 IPQ 206, 221.
[49] Shin-yi Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) J Int Economic Law 18(2) 449, 468.
[50] Peter Van den Bossche and Sarah Akpofure, 'The Use and Abuse of the National Security Exception under Article XXI(b)(iii) of the GATT 1994', WTI Working Paper No. 03/2020, 5-6, https://www.wti.org/research/publications/1299/the-use-and-abuse-of-the-national-security-exception-under-article-xxibiii-of-the-gatt-1994/ accessed 1 July 2025.
[51] Neha Mishra, *International Trade Law and Global Data Governance: Aligning Perspectives and Practices* (Hart, 2024) 92.

Economic and Social Research Council

rights and obligations of various stakeholders as well as promoting the public interest in critical sectors in society.