How to cite this paper:

Cuomo, F. (2024). Europe's Export of Cybersurveillance Technology: Impacts on Myanmar's Civil Society. *Perspective Politice*. Pages [79-88].

https://doi.org/10.25019/perspol/24.17.0.8

Article

Europe's Export of Cybersurveillance Technology: Impacts on Myanmar's Civil Society

Abstract: *This contribution aimed to examine the critical issues related to the export of cybersurveillance technologies by some European Union companies to Myanmar, a country with a history of instability and geopolitical tensions that have been exacerbated since the military coup of 2021. Non-governmental organizations operating in the country, in addition to humanitarian and development assistance, play a crucial role in the evolution of civil society, and, also thanks to some of them, it has been possible to find out some irregularities in the export of dual-use goods that may cause social impacts and infringe on the freedoms of Burmese civil society.*

Through a qualitative analysis of the literature, the main EU regulations, and related NGOs documents, the research uncovered some regulatory loopholes that allowed such exports while examining the practices of some European companies in Burma.

The work carried out confirmed the need for stricter regulation: in this sense, the European Commission's recent Delegated Regulation 2023/66 aims to ensure more effective control over this type of export by preventing the misuse of surveillance technology and promoting greater accountability of companies operating in authoritarian contexts.

Keywords: *civil society, dual-use goods, NGOs, mass surveillance, social impacts.*

Federico CUOMO

Department of Humanities and Social Sciences, University of Sassari, Researcher, Italy;
ORCID: 0009-0006-9042-0595;
fcuomo@uniss.it

1. Introduction

The export of advanced surveillance technologies from Europe to countries with undemocratic regimes and the potential contribution of the EU to surveillance activities beyond its borders (Kanetache, 2019) is a debated topic in light of recent international tensions. Already more than a decade ago, Edward Snowden's revelations (so-called *whistleblowing* – The Washington Post, 2019) had sensitised institutions and citizens on the risks of mass surveillance, highlighting the importance of protecting data privacy and observing strict rules for the import and export of foreign technologies in order to reduce social impacts on civil society.

This contribution aims at highlighting some critical aspects of the EU Regulation 2021/821 (and of the previous one 2009/428) concerning the export of dual-use items[1], i.e. goods for civil use but potentially usable also for military purposes; the European Union's will to overcome these weaknesses has led to the recent Delegated Regulation 2023/66 of the European Commission (Fig. 1), which came into force on 12 January 2023, introduced precisely to strengthen the rules and sanctions governing this type of export, in response to the numerous reports on the misuse of technologies exported by the EU to third countries.

Fig. 1. Front page of EU Commission Delegated Regulation 2023/66 of 21 October 2022

11.1.2023 EN Official Journal of the European Union L 9/1

COMMISSION DELEGATED REGULATION (EU) 2023/66

of 21 October 2022

amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items ([1]), and in particular Article 17(1) thereof,

Whereas:

(1) Regulation (EU) 2021/821 requires dual-use items to be subject to effective control when they are exported from or in transit through the Union, or are delivered to a third country as a result of brokering services provided by a broker resident or established in the Union.

(2) Annex I to Regulation (EU) 2021/821 establishes the common list of dual-use items that are subject to controls in the Union. Decisions on the items subject to controls are taken within the framework of internationally agreed dual-use controls.

(3) The list of dual-use items set out in Annex I to Regulation (EU) 2021/821 needs to be updated regularly in order to ensure full compliance with international security obligations, to guarantee transparency, and to maintain the competitiveness of economic operators. The control lists adopted by the international non-proliferation regimes and export control arrangements have been changed during 2021, and therefore Annex I to Regulation (EU) 2021/821 should be amended accordingly. In order to facilitate references for export control authorities and economic operators, Annex I to that Regulation should be replaced.

(4) Regulation (EU) 2021/821 empowers the Commission to update the list of dual-use items set out in Annex I by means of delegated acts, in conformity with the relevant obligations and commitments, and any amendment thereof, that Member States and, where applicable, the Union have accepted as members of the international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties.

(5) Considering the importance of ensuring full compliance with international security obligations as soon as practically possible, this Regulation should enter into force on the day following that of its publication.

A captious interpretation of some regulations has allowed some documented cases of exports and subsequent misuse by authoritarian regimes; an example of this is the involvement of EU-based companies in the supply of surveillance technology to the Burmese military government, revealed by some non-governmental organizations (NGOs) and independent investigations in 2021[2]. In the country, political instability and inflation are squeezing the already low incomes of the poorest families; a crisis situation that is worsening and threatening an entire segment of Myanmar's population (Terre des Hommes, 2024). Moreover, the authoritarian breakthrough following the military coup in February 2021 has reopened the debate on the use of information technology in Myanmar and the provision of technology support by EU companies.

This research, after analysing the existing literature and European legislation on the subject, examined the main publications related to the aforementioned investigation that revealed some "opaque" export transactions between some European technology companies and the Burmese military regime. An intentional sampling methodology was used, leading to a qualitative analysis of various documents, published between 2021 and 2023, from NGOs, news channels, and independent investigations.

2. Literature analysis and EU regulations

In the literature, cybersurveillance eludes a univocal description, as the concept can extend to a wide range of objects and technologies; this is either because definitions are "list-based" (Vila Seoane, 2020), or because these are "emerging technologies" that are constantly evolving (Kim, 2021), or because the definition varies from country to country, depending on security institutions and standards (XI Meeting of the Chaudfontaine Group, 2022). Not even the European Union has adopted a precise definition for digital surveillance, which, however, is included in the broader category of dual-use technologies under the regulations that provide member countries with a framework of rules, codes of conduct, and procedures for export (Meissner and Urbanski, 2022), highlighting the complexity and delicacy of the issue at the international level. The term dual-use refers to objects or software that can be used for both civil and military purposes (Regulation 2021/821, Article 2.1), but this civil-military dichotomy is not always evident when it comes to the regulation of surveillance technologies. This is because the modification of security tools into real surveillance weapons is not particularly complex for private industries that have the resources and expertise to produce both (Vila Seoane, 2020); cyber technologies therefore have the potential to be misused, regardless of their original intention.

EU Regulation 2009/428, the basis for the export of dual-use technologies, has been subject to several legal revisions (Bromley and Brockmann, 2021), highlighting the Union's ongoing efforts to adapt regulations to the evolving technological and security landscape.

The 2009/428 inherited some elements from previous post-war international institutions, including *The Wassenaar Arrangement* (1996[2023]) and the *COordinating COmmittee for Multilateral export control* (1945) (see Yasuhara 1991), having non-proliferation of arms as a common goal (Meissner and Urbanski, 2022). The Wassenaar Arrangement (WA) is a multilateral agreement to control the export of conventional arms, dual-use materials, and technologies to contribute to regional and international stability and security; the technical and diplomatic activities of this body (which is based in Vienna and to which 40 countries adhere) aim to harmonise and make more transparent the export and control policies of Member States on the aforementioned exports, with the aim of limiting the accumulation of conventional armaments in areas considered to be at risk. This regime succeeds the COordinating COmmittee for Multilateral export control (COCOM), which, after the end of the Cold War, used mechanisms that were clearly outdated by the course of historical events.

The review process undertaken in 2011 developed out of the need to broaden the reasoning and justification of the EU regulation (Lavallée, 2018). In 2016, there is a "regulatory shift" in the legal nature of regulation (Kanetake, 2019); whereas the essential purpose of the 2009 regulation was military risk mitigation, in accordance with the WA, the 2016 proposal (European Commission 2016/0295) highlights that regulation on the export of dual-use items is necessary

to protect civil liberties and human rights (Lubin, 2023; Kyaw, 2020) of civil society. This regulatory change can be traced back to the revolts that took place in the Middle East and North Africa (MENA) regions between 2010 and 2012, known as the "Arab Spring"; various reports by NGOs and international organisations had shown the support offered by EU-based companies to authoritarian regimes to build a surveillance system aimed at suppressing protests.

The 2016 reform focused on the creation of an autonomous list, not based on other international regimes, which would include cybersurveillance tools in a specific category of dual-use goods (Group 10) and deepened the obligation of private companies to exercise due diligence[3], inserting a clause obliging Member States to identify potential human rights damages caused by dual-use technologies (Vila Seoane, 2020) and inform the Commission (2016/0295, Article 4, para. 2), in order to reduce social impacts on civil society by defining the failure of exporters to inform as negligence; finally, the reform emphasises the need for greater alignment and coordination between Member States. A number of scholars have pointed out that the Commission's 2016 proposal aimed to harmonise the enforcement of Member States' export restrictions by clarifying key terms, standardising controls and promoting uniformity of export restrictions and enforcement measures (Bromley and Brockmann, 2021).

Based on these precedents, Regulation 2021/821 was developed, which represents a further step towards the creation of an autonomous EU framework for the detection and control of surveillance instruments, aiming at greater clarity and improved cooperation between Member States and exporting companies. However, some scholars (Meissner and Urbanski, 2022) provide a critical analysis of Regulation 2021, pointing out its weaknesses. Although the regulation is binding, it grants Member States some flexibility in adapting it, which has led to divergent interpretations between countries, particularly with regard to penalties for the export of dual-use items. There also appears to be a divergence in the interpretation and application of the checklist, annexed to the regulation, which specifies the licensing criteria. The authors attribute this inconsistent implementation by national authorities to a combination of factors, including institutional arrangements, resources, size, and competencies.

Recent ongoing wars in the international chessboard have generated an acceleration of the regulatory process, leading to the new EU Delegated Regulation 2023/66, which aimed to strengthen controls on the export of dual-use items by amending Regulation 2021/821 on the list of those items. The Regulation includes Annex I (Fig. 2) which contains the list of dual-use items and is updated annually to take into account new technologies and threats.

This is, thus, the current legal text to be considered in order to carry out objective verifications to determine whether an item or technology is dual-use and, if so, whether it is subject to export authorisation. Transactions subject to control under the Regulation include export but also brokering services, technical assistance, transit and transfer of dual-use items.

The European Union, in the context of the Common Foreign and Security Policy (CFSP), implements restrictive measures to achieve the objectives set out in the Treaty on European Union. In recent years, the EU has frequently resorted to sanctions or restrictions either autonomously or in accordance with binding UN Security Council resolutions. Such measures may be directed against governments of third countries as well as non-state entities and natural or legal persons, such as terrorist groups or individual terrorists; restrictions may include arms embargoes, specific or general trade restrictions (such as import or export bans, and others). Each Member State identifies a competent body to implement the measures established by the

United Nations and the European Union to oversee the functioning of the system for preventing and combating:

– the financing of terrorism and money laundering;
– the activities of countries that threaten international peace and security;
– the financing of the proliferation of weapons of mass destruction.

Fig. 2. The dual-use categories. Source: EU Delegated Regulation 2023/66, Annex I

'ANNEX I

LIST OF DUAL-USE ITEMS REFERRED TO IN ARTICLE 3 OF THIS REGULATION

The list of dual-use items contained in this Annex implements internationally agreed dual-use controls including the Australia Group (1), the Missile Technology Control Regime (MTCR) (2), the Nuclear Suppliers Group (NSG) (3), the Wassenaar Arrangement (4) and the Chemical Weapons Convention (CWC) (5).

CONTENTS

At present, trade restrictions are in place against the following countries: Afghanistan, Belarus, Bosnia Herzegovina, Burundi, Central African Republic, China, Congo, North Korea, Guinea, Guinea-Bissau, Haiti, Iran, Iraq, Lebanon, Libya, Mali, Moldova, Montenegro, Myanmar, Nicaragua, Russia, Serbia, Somalia, Sudan, South Sudan, Syria, Tunisia, Turkey, Ukraine, United States, Venezuela, Yemen, Zimbabwe.

3. Europe's exports to Myanmar and NGOs

With a history of disorders and geopolitical conflicts, marked by the coup d'état of 2021 with the takeover of power by the military junta, Myanmar (on the list of trade-restricted countries) is a salient context for analysing EU exports of surveillance technology to countries with authoritarian regimes.

Following the 2021 investigation of the so-called "Myanmar controversy" (The Lighthouse Reports, 2021), other NGOs also examined the export activities of European companies supplying surveillance technology to the Burmese military authority. This research focused, in particular, on eight documents issued by seven different organisations concerning three European companies producing surveillance equipment: the Swedish MSAB, the Italian SecurCube, and the Norwegian Telenor. The documents examined reveal that, between 2018 and 2021, the Burmese military allegedly acquired advanced investigation and surveillance technology with the aim of "extracting data from smartphones, accessing phone conversations and monitoring people's movements" (Maizland, 2022).

It seems likely that the *Tatmadaw* (the Burmese Armed Forces – Campbell and Chandler, 2021) has acquired technology from the MSAB that can retrieve call logs, passwords, contacts, personal data, messages, GPS data and other records. The company claimed, first of all, that it had duly obtained licences to export the technology from the Swedish regulators in 2018, an assertion in accordance with EU guidelines that state that each Member State must grant export licences through its national regulators (Meissner and Urbanski, 2022) and, furthermore, that the licences could have been granted because the exported technologies were not – officially – capable of breaking a phone's encryption. The licences had been conceded before the embargo came into force in 2018[4], only to be revoked in 2021 when the political situation in Myanmar precipitated. A final argument in favour of the legal legitimacy of the MSAB's exports is that the negotiations had been concluded before the military coup and after the democratic elections of 2015, when the country was led by Aung San Suu Kyi, winner of the Nobel Peace Prize, and therefore considered de jure a democracy (ISPI, 2021). In summary, despite the doubts, the export of the MSAB's technologies was approved because the company had successfully completed the bureaucratic procedures required by Swedish law, the structure of the exported technology did not infringe on the right to privacy, and, most importantly, the transaction was completed at a time when Myanmar was considered de facto a democracy.

There are reports of exports of IT forensic tools by Italy's SecurCube to Myanmar; in particular, the export to the country of the BTS tracker, a tool capable of capturing and decoding call logs, text messages, multimedia messages, and location information. The company declined to comment on these reports, merely stating that it is solely up to the national authority to decide on the export of such technology. It was verified that while no documentation could prove a direct export of the BTS technology (IrpiMedia, 2022), an indirect export (so-called triangulation) may have taken place, meaning a European manufacturer selling technology to authorised countries who, acting as intermediaries, subsequently resell the goods to an embargoed country (Justice for Myanmar, 2023).

According to an NGO working on the territory, the Norwegian company Telenor provided telecommunications services to Myanmar from 2014 to 2021, when it left the country following the military coup (Access Now, 2023). Instead, according to the company, the Burmese military left it no choice but to sell all assets; if it had remained in the country, it would have

been forced to cooperate with the Burmese authorities and install eavesdropping software (IrpiMedia, 2021; Euronews, 2022). Investigations revealed that the Norwegian company had purchased an interception gateway from China and installed it in its systems, thus violating sanctions imposed by the EU and Norway (Thompson, 2022; Myanmar Now, 2022). Furthermore, the company came under the spotlight because of its decision to sell all assets (including licences, infrastructure, employees and customers), including the interception gateway, to the M1 Group (Euronews, 2022), but information from NGOs revealed that the M1 Group is a Lebanese company with a history of operating in authoritarian countries, lacking respect for international human rights standards (Access Now, 2023). In this context, Telenor was accused of violating the right to privacy according to the European General Data Protection Regulation; by selling to the M1 Group, it could no longer guarantee the protection of its customers' data (Euronews, 2022).

4. Loopholes in EU regulation

In the following, we examine the three above-mentioned company cases from the perspective of the relevant EU regulations in order to highlight some relevant regulatory ambiguities.

As mentioned, the Swedish government had granted the company MSAB a licence to export its surveillance technology in 2018, consistent with EU Regulation 2021/821, an example of "collective governance" in which relevant decisions are not assessed within the European framework but delegated to member states (XI Meeting of the Chaudfontaine Group, 2022). However, by returning decision-making power to the member states, the regulation favours a non-universal application of the law that is subject to the assessments of individual states, rather than an EU directive. The other Member States have no title in the Swedish licensing bodies' control procedures (Meissner and Urbanski, 2022), where the act of returning decision-making power highlights an ineffective dual sphere of action between Europe and the member states. Today, in fact, in the Union, where trade policy is a common matter, the regime is the same for all countries, but each member state has its own national authority to oversee it. Furthermore, MSAB was able to defend the export of dual-use technology by arguing that it had no ability to circumvent the encryption of a phone, whereas forcing the user to hand over certain information made it possible to extract sensitive data (Kyaw, 2020). Therefore, the tool could be exported as it did not appear to be designed to "allow intrusion" (as indicated by contribution 8 of EU regulation 2021/821), but the definition of surveillance tools did not consider that the possible harm caused by cybersurveillance technologies does not depend only on their design but also on the subsequent way in which the tool is used. Finally, in the MSAB case, a further definitional criticality emerges in relation to the interpretation of the concept of a democratic state. The company argued that it acted legally because it sold its technologies to Myanmar during a period when the country had a de jure democratic government (ISPI, 2021). However, a broader analysis of the political situation between 2015 and 2021 reveals, despite the democratic label, instability and serious violations (such as the genocide of the Rohingya committed by the Burmese military), where paragraph 2 of the EU regulation explicitly prohibits the export of dual-use items in cases of human rights violations. Thus, MSAB's justification for exporting to Myanmar denotes a practice of regulatory arbitrage, as the company invoked the de facto democratic institutional set-up of the former Burma instead of recognising the authoritarian nature of the military junta.

A further example of such regulatory ambiguity is the SecurCube case; as mentioned, the company refused to explain how the surveillance technology got into the hands of the Burmese army, while it is plausible that the goods were triangulated through a third country (ISPI, 2021; Justice for Myanmar, 2023). By this expedient, the company, but also the Italian institutions[5], can claim that the goods were exported in compliance with the applicable rules, nor do European regulations provide for any liability on the part of state authorities in the case of triangulation. In this case, not even the principle of due diligence, which stipulates that companies must inform the Commission if they are aware of violations caused by their products, succeeds in attributing more responsibility; it is extremely difficult, in fact, to monitor the level of awareness of companies regarding the implications on civil liberties resulting from the use of their products. Therefore, the SecurCube case highlights the need for a regulatory system that favours the monitoring of cybertechnology exports throughout the entire life cycle, from purchase to possible subsequent resale.

The Telenor case highlights a further example of regulatory arbitrage in the application of EU export law. The company's decision to exit the market was motivated by a willingness to not comply with the demands of the Burmese military government that would have violated not only European regulations, but also the rights of the company's customers. However, the simultaneous decision to sell all assets determined the entry into the Burmese market of Group M1, a company with a long history of violating human rights regulations. A further loophole is thus revealed: the European regulation includes provisions restricting the export of dual-use items to certain countries, but does not elaborate on the possible repercussions of leaving the markets of authoritarian countries.

5. Conclusions

This paper aimed to investigate, through a qualitative analysis of European regulations, NGO and independent documents, the export of cybersurveillance technology and dual-use goods by EU companies to Myanmar.

The research revealed some weaknesses in the EU regulations for such exports, at least until the beginning of 2023, including overlapping competences at the national and European levels, complexity in performing and complying with due diligence assessments, arbitrary interpretation of definitions, regulatory arbitration practices, and regulatory gaps. The dual sphere of action between the national and the European level appears to be a factor of weakness: on the one side, legislation provides a framework of common rules for the export of surveillance technology; on the other side, the Union returns operational responsibility to the Member States, allowing for an enforcement of the law that depends on national institutions and their interpretations. Research has highlighted the complexity for private companies in complying with due diligence, and this is due to the fact that regulations are unclear in defining the liability of companies themselves for damages caused by their technology. The relevant EU regulations allow for sometimes arbitrary interpretations of the definitions: one case of regulatory arbitrage was observed where a company had selectively applied only the favourable parts of the regulations while circumventing others in order to export surveillance technology.

If it appears complex to balance the economic interests of companies with those of civil society, the work of NGOs and the results of the research point to an aspiration for a legitimate strengthening of regulations on the export of cybersurveillance and dual-use technology in author-

itarian contexts; it is to be expected, therefore, that the European Commission's new EU Delegated Regulation 2023/66, which was created to tighten regulations and controls, can best deploy its effects by mitigating any potential impact of such exports on human rights and civil liberties.

Notes

1. Dual-use goods are products, consisting of both tangible and intangible assets, such as software, designs and technologies, which, although created and sold for civil use, in industry, medicine or scientific research, can also be used for military purposes or for the production of weapons of mass destruction. Such products differ from weapons materials in that they are not specially designed for military use but could also be used for this purpose. These are common goods and technologies such as valves, pumps, computers, electronic materials, sensors and lasers, avionics, shipbuilding, aerospace, machinery, vehicles, chemicals, metals, electrical equipment, etc., but with high technological content (Commission Delegated Regulation, 2022).

2. Access Now (2023) is an NGO and Lighthouse Reports (2021) an investigative journalism team that works with the world's leading media to carry out public interest investigations.

3. Principle established in the 2016 European reform and reinforced in contribution 5 of the 2021 review.

4. The embargo banned the export of surveillance products to Myanmar because of human rights violations.

5. The competent national authority in Italy is the UAMA (Unit for the Authorisation of Armament Materials), which is part of the Ministry of Foreign Affairs and International Cooperation (Ministero italiano degli Affari Esteri e della Cooperazione Internazionale, 2024).

Conflicts of interest

The author declares no conflict of interest.

References

Access Now (2023) *As Myanmar junta extends control over telcos, surveillance and privacy risks increase*. Available at: https://accessnow.org/press-release/myanmar-junta-surveillance-telcos.

Bromley, M. and Brockmann, K. (2021) *Implementing the 2021 Recast of the EU Dual use Regulation: Challenges and Opportunities*, Stockholm International Peace Research Institute.

Campbell, Z. and Chandler, C. L. (2021) *Tools for repression in Myanmar expose gap between EU tech investment and regulation*. Available at: https://theintercept.com/2021/06/14/myanmar-msab-eu-technology-regulation.

Commission Delegated Regulation, EU (2022) Regulation 2023/66, 2021/821, 2016/0295. Available at: https://eur-lex.europa.eu.

Euronews (2022) *Norway can't stop transfer of Telenor data to Myanmar rulers-minister*. Available at: https://euronews.com/2022/02/16/us-myanmar-telenor-norway.

IrpiMedia (2021) *L'export dei software di sorveglianza fra triangolazioni e opacità*. Available at: https://irpimedia.irpi.eu/euarms-myanmar-export-dual-use-triangolazioni.

IrpiMedia (2022) *Myanmar, lo stato di sorveglianza che aggira l'embargo della U.E.* Available at: https://irpimedia.irpi.eu/euarms-armi-dual-use-birmania.

ISPI (2021) *L'esercito del Myanmar vuole prendersi il paese costi quel che costi*. Available at: https://ispionline.it/it/pubblicazione/lesercito-del-myanmar-vuole-prendersi-il-paese-costi-quel-che-costi-31137.

Justice for Myanmar (2023) *Telenor Group violating sanctions through installation and imminent transfer of German Lawful Intercept Gateway*. Available at: https://justiceformyanmar.org/press-releases/telenor-group-violating-sanctions– through-installation-and-imminent-transfer-of-german-lawful-intercept-gateway.

Kanetake, M. (2019) The EU's dual-use export control and human rights risks: the case of cyber surveillance technology. *Europe and the World: A law review*, 2-13.

Kim, H. J. (2021) Global export controls of cyber surveillance technology and the disrupted triangular dialogue. *International and Comparative Law Quarterly*, Cambridge University Press, 379-415.

Kyaw, P. (2020) *The rise of online censorship and surveillance in Myanmar*. Open Technology Fund.

Lavallée, C. (2018) The EU's dual-use exports: a human security approach? Chaillot Papers, *European Union Institute for Security Studies (EUISS)*, 43-50.

Lubin, A. (2023) *Selling Surveillance*, Research Paper No. 495, Indiana Legal Studies.

Maizland, L. (2022) *Myanmar's troubled history: coups, military rule, and ethnic conflict*. Council on Foreign Relations, 31.

Meissner, K. L. and Urbanski, K. (2022). Feeble rules: one dual-use sanctions regime, multiple ways of implementation and application? *European Security*, 222-241.

Ministero italiano degli Affari Esteri e della Cooperazione Internazionale (2024) *Come esportare beni dual-use*. Available at: https://export.gov.it/news-e-media/news/come-esportare-beni-dual-use.

Myanmar Now (2022) *Norway's Telenor accused of 'egregious breach' of EU sanctions*. Available at: https://myanmar-now.org/en/news/norways-telenor-accused-of-egregious-breach-of-eu-sanctions-with-surveillance-system-that-will-allow-myanmar-junta-to-spy-on-millions.

Terre des Hommes (2024) *Together against malnutrition in Myanmar*. Available at: https://tdh.org/en/together-against-malnutrition-in-myanmar.

The Lighthouse Reports (2021) *EU Spy Tech in Myanmar – EU funds and techn secretly aid junta in spying on Burmese*. Available at: https://lighthousereports.com/investigation/eu-spy-tech-serves-myanmar-junta.

The Washington Post (2013) *Edward Snowden says motive behind leaks was to expose surveillance state*. Available at: https://washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html.

The Wassenaar Arrangement (2023) *Origin*. Available at: https://wassenaar.org/about-us.

Thompson, C. (2022) *Norwegian telecoms company faces privacy complaint over sale of Myanmar subsidiary*. Available at: https://codastory.com/authoritarian-tech/myanmar-telenor-gdpr.

Vila Seoane, M. (2020) Normative Market Europe? The Contested Governance of Cyber-surveillance Technologies. In A. Calcara, R: Csernatoni and C. Lavallée, eds. *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*. Routledge.

XI Meeting of the Chaudfontaine Group (2022). *How the new EU Dual use Regulation could benefit third countries?* European Studies Unit (ESU), University of Liège. Available at: https://esu.ulg.ac.be/new-publication-how-the-new-eu-dual-use-regulation-could-benefit-third-countries.

Yasuhara, Y. (1991) The Myth of Free Trade: The Origins of COCOM 1945–1950. *The Japanese Journal of American Studies*. Available at: https://jaas.gr.jp/jjas/pdf/1991/No.04-127.pdf.