

Scenario 26: Export licensing of intrusion tools

Two different States licensed exports of intrusion tools and related items to a third State. That State then used it to spy on human rights defenders, lawyers, journalists, activists,



© BiljanaJovanovic. Licensed Image by Pixabay

opposition politicians, and dissidents. While one of the licensing States is a member of the Wassenaar Arrangement, the other is not but had declared to follow it unilaterally. The legal analysis considers the attribution of the relevant acts and omissions by the States and examines possible breaches of international export control law and international human rights law.

Contents

Scenario

Keywords

Facts

Examples

Legal analysis

Attribution

[Breach of international obligation](#)

[Export control obligations of State A](#)

[Export control obligations of State B](#)

[Human rights obligations of State C](#)

[Human rights obligations of State A and B](#)

[Checklist](#)

[Appendixes](#)

[See also](#)

[Notes and references](#)

[Bibliography and further reading](#)

[Contributions](#)

Scenario

Keywords

Complicity, due diligence, international export control law, international human rights law, surveillance, unilateral declarations

Facts

[F1] Private technology firms incorporated in States A and B develop smartphone intrusion tools and sell those tools to foreign governments. The tools can be installed silently on smartphones of specific target persons. The intrusion happens without the affected person's knowledge, using so-called zero-touch zero-day vulnerabilities. After successful intrusion, the tools can be used to access and copy the smartphone's data, communications, and photos and turn on the microphone, camera, and GPS tracking. In addition, they can be used to detect with whom the target person has met.

[F2] The domestic laws of States A and B required a prior export licence for the export of such tools and related items. Accordingly, the export control agencies of States A and B licensed each export of the tool to State C's government, as well as each export of related

items (**incident 1**). Within the licensing process, domestic law required the agencies to assess the human rights risks associated with such exports, which they did.

[F3] Once licensed, the firms transferred the tools and related items to State C's government (**incident 2**).

[F4] The law enforcement and security agencies of State C used the tool not only to fight crime and terrorism but also to domestically spy on human rights defenders, lawyers, journalists, activists, opposition politicians, and dissidents (**incident 3**). This was revealed by an investigative research project conducted by multiple news outlets and NGOs.

[F5] After the export control agencies in States A and B became aware of these facts, they immediately revoked all export licences for the tools and related items to State C.

[F6] States A, B, and C are United Nations member States and parties to the International Covenant on Civil and Political Rights (ICCPR). Moreover, State A is a participating State in the Wassenaar Arrangement (WA) and incorporated it into its domestic law and policies. State B is not a participating State. However, in a public written statement, the president and head of government of State B had expressly pledged that State B would comply with the WA and the related documents. Moreover, the statement calls on other States to hold State B accountable for its pledge. Following the announcement, State B aligned its laws and export control policies with the WA and the related documents.

Examples

- [The Hacking Team Hack \(2015\)](#)
- [Ethiopian surveillance of journalists abroad \(2017\)](#)
- [Pegasus Project revelations \(2021\)](#)

Legal analysis

For a general overview of the structure of analysis in this section, see [Note on the structure of articles](#).

[L1] The legal analysis in this scenario first considers which relevant conduct is attributable to the States concerned. Then it examines whether that conduct amounts to a breach of international obligations incumbent on those States.

Attribution

State organs and persons and entities in exercise of governmental authority [Collapse]



The following types of conduct of State organs and persons and entities in exercise of governmental authority are attributable to a State:

1. The conduct of any of the organs of that State, "whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State";^[1]
2. The conduct of an organ of another State placed at the disposal of the State in question, if "the organ is acting in the exercise of elements of the governmental authority" of the latter State;^[2]
3. The conduct of "a person or entity which is not an organ of the State [...] but which is empowered by the law of that State to exercise elements of the governmental authority, [...] provided the person or entity is acting in that capacity in the particular instance."^[3]

Such conduct is attributable to the State even if the organ, person or entity acting in that capacity "exceeds its authority or contravenes instructions" (acts *ultra vires*).^[4]

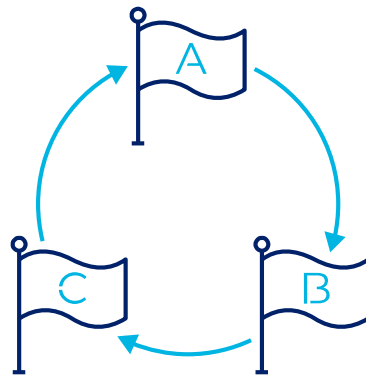
[L2] Incident 1 (licensing the export of the surveillance tools): State A's and State B's export control agencies approved and licensed each export. They are State organs of States A and B, respectively. Therefore, issuing the export licences can be attributed to States A and B.

[L3] Incident 3 (use of tools against human rights activists and opposition): State organs of State C used the intrusion tool domestically against human rights defenders, lawyers, journalists, activists, opposition politicians, and dissidents. Thus, the use of the tool can be attributed to State C.

[L4] By contrast, State C's use of the tool cannot be attributed to States A and B as their own conduct, as it was not carried out by their State organs. However, it is debatable whether States A and B

may have aided and assisted importing State C by granting the export licences, to which the analysis now turns.

Responsibility of a State for the conduct of another State [Collapse]



A **joint or collective wrongful act** may result in a plurality of responsible States.^[5] According to the principle of independent responsibility, each State is responsible for its own internationally wrongful conduct.^[6] However, a State may also be responsible for a wrongful act of another State if it is implicated in the

conduct of the latter. International law recognizes several forms of derived international responsibility:^[7]

- **Aid or assistance** with a view to assisting in the commission of a wrongful act by another State;^[8]
- **Direction or control** over the commission of an internationally wrongful act of another State;^[9]
- **Coercion** of another State into the commission of an internationally wrongful act.^[10]

These forms of implication have in common that the specific nature of the relationship between the State that is the actual author of the unlawful act and the implicated State causes the incurrance of responsibility of the latter.^[11]

The assisting State will typically not be responsible for the assisted wrongful act^[12] but for a distinct wrongful act – i.e., for deliberately assisting another State in breaching an international obligation by which they are both bound.^[13] In contrast, the exercise of direction and control or coercion by one State over the commission of an internationally wrongful act by another incurs responsibility for the act itself^[14] towards the injured State.^[15] The coerced State might benefit from *force majeure* if the requirements are met.^[16] In that case, it would be solely the State exerting coercion that would bear responsibility.^[17]

[L5] There is no indication that State A's or State B's export control agency, or any other organ of those States, knew how State C would use the tool when they issued the export licences. Moreover, there is no indication that the export control agencies did so with a view to assisting other States in the commission of a wrongful act by using the tool. Constructive knowledge ("should have known") on State A's or State B's side does not suffice to hold those States responsible for aiding and assisting.^[18]

Non-State actors

[Collapse]



Activities of non-State actors (groups and individuals) are generally not attributable to States. However, such conduct can be attributable to a State in particular if the actor is:

1. "in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct";^[19]
2. "in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority";^[20]
3. "an insurrectional movement which becomes the new Government of a State";^[21] or
4. "a movement, insurrectional or other, which succeeds in establishing a new State in part of the territory of a pre-existing State or in a territory under its administration".^[22]

Additionally,

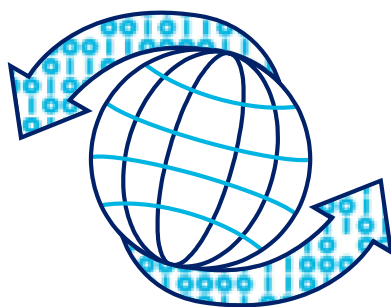
- 1.
5. the conduct of a non-State actor is attributable to a State "if and to the extent that the State acknowledges and adopts the conduct in question as its own".^[23]

[L6] **Incident 2** (sale of the tools by the companies): Under certain circumstances, the conduct of non-State actors is attributable to States. Thus, the question arises whether the actual transfer of the tools and related items by the private companies to State C is attributable to States A and B.

[L7] Although each export required a prior licence by States A and B, respectively, that does not suffice to bring the respective companies under the direction or control of the licensing States.^[24] Instead, it must be considered whether the companies acted with the authorization of their respective States in the sense of Article 5 ARSIWA. Article 5 ARSIWA applies to the authorization of the exercise of governmental authority by non-State actors.^[25] The export licensing, which is an exercise of governmental authority, was done by the organs of States A and B and not by the private companies. The latter engaged only in sale and transfer, which is not an exercise of governmental authority. Moreover, the companies were not acting in the name or on behalf of their States of incorporation. Hence, the companies' sale and transfer of the tools are not attributable to State A or State B.

Breach of international obligation

Export control obligations of State A



International export control law has three main pillars: binding international arms treaties,^[26] UN Security Council resolutions, and non-binding multilateral export control regimes.^[27] Among these, only the Wassenaar Arrangement (WA) deals with cyber tools.

The WA is a non-binding export control regime with 42 participating States as of 2022,^[28] many of which have a significant cyber technology sector. Moreover, some non-participating States align their export control legislation and policies – partially or wholly – with the WA.^[29]

The WA's primary goal is “to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations.”^[30] To this end, the participating States should apply export controls to every item on the WA's Dual-Use or Munitions List.^[31] Both lists have been amended to include specific cyber tools and related items to prevent destabilizing accumulations of these items, thereby contributing to security and stability in cyber space.^[32]

The Munitions List designates “‘Software’ specially designed or modified for the conduct of military offensive cyber operations”^[33] as a controlled item.^[34] Furthermore, the list covers the technology related to such software.^[35]

The Dual-Use List deals with cyber intrusion tools. However, the WA does not place intrusion tools themselves on the Dual-Use List but only items related to intrusion tools.^[36] Whereas an “intrusion tool” means the actual “intruding” software that is installed on the target device, related items are “systems, equipment, and components” or “‘software’ specially designed or modified for the generation, command and control, or delivery of ‘intrusion software’”.^[37]

Moreover, States agreed to follow certain best practices to control the transfer of said cyber items irrespective of their means of transfer, thus, including their intangible transfer such as via e-mail or the cloud.^[38]

Consequently, participating States should require a prior export licence for each export of a cyber tool or related items covered by the WA. In the licensing process, the export control agency should examine whether the transfer of such cyber items would contribute to destabilizing accumulations. There is no clear definition within the WA and no consensus among the participating States on what constitutes “destabilizing accumulations”. Nevertheless, the regime includes best practices setting out relevant elements States should consider in their assessment, at least with respect to weapons.^[39] Human rights concerns are included among the elements to consider.^[40] However, the final licensing decision always remains within the sole discretion of each participating State.^[41]

[L8] Since the WA is non-binding, non-compliance by a participating State does not constitute a breach of an international obligation. Thus, State A did not breach any international law obligation in this respect.

Export control obligations of State B

[L9] State B might have breached its international export control obligations. Although State B is not a participating State in the WA, it has declared to follow the WA unilaterally. Therefore, the question arises whether the WA’s requirements have become binding on State B by means of its unilateral declaration.

Legally binding unilateral declarations of States

[Collapse]



Under certain circumstances, a unilateral declaration of a State may give rise to legally binding obligations onto the declaring State.^[42] The binding character of such a declaration is based on the principle of good faith.^[43]

States regularly resort to unilateral declarations in the cyber context, including declarations on the possible content of confidence-building measures for cyber space,^[44] declarations of disapproval regarding specific cyber behaviour by other States,^[45] declarations regarding the attribution of specific cyber attacks, and national position papers on cyber space.^[46] It is, however, doubtful that these declarations fulfil the criteria for binding unilateral declarations.

For a unilateral declaration to be legally binding, the following criteria must be met:

1. The declaration must be made publicly.^[47] It may be expressed either in oral or written form.^[48] The declaration may be addressed to a specific subject of international law, i.e., a State, or to the international community as a whole.^[49]
2. The declaration must express the will of the declaring State to be bound by the declaration.^[50] To determine whether a declaration is binding, its content, all the factual circumstances in which it was made, and the reactions to which it gave rise must be considered.^[51]
3. The declaring state organ must be authorized to make the according declaration,^[52] as is presumed for heads of State, heads of Government, and ministers for foreign affairs.^[53]
4. The content of the declaration must be sufficiently clear and specific.^[54] The obligations themselves must be interpreted primarily considering the text together with the context and the circumstances in which it was formulated.^[55] In case of doubt, a restrictive interpretation should be chosen.^[56]

[L10] Firstly, State B's declaration must meet the criteria of a binding unilateral declaration. State B made the unilateral declaration publicly and addressed it to the international community as a whole. It was made by the president and head of government of State B. Moreover, it expressly stated that State B would comply with the WA, and that other States may hold State B accountable. Thus, the phrasing of the unilateral declaration expresses the will of State B to be bound by its declaration. Therefore, the unilateral declaration can be considered binding.

[L11] Secondly, the binding content of the declaration must be determined. The declaration transforms the non-binding requirements of the WA into binding international law obligations for State B.^[57] Consequently, State B is, among other duties, obliged to establish export controls for the items listed on the WA's lists, probe whether a licence needs to be denied to prevent destabilizing accumulations, and follow the relevant best practices.

[L12] Thirdly, State B must have breached one of the obligations just set out. Intrusion tools themselves are not among the items listed, but exports of items related to the intrusion tools are and, therefore, must be controlled by State B.^[58] Accordingly, State B's export control legislation required a prior licence for each export of such items. In fact, State B licensed each export of the tools and related items by its companies. Furthermore, there is no indication that its export control system was not in compliance with the best practices of the WA regarding transfers of intangible items.

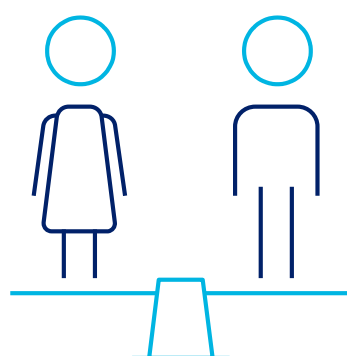
[L13] Finally, State B was obliged to consider for each export licence application whether the export would contribute to destabilizing accumulations and, on that basis, would not be eligible for an export licence. However, this decision always remains within the sole discretion of State B.^[59] By issuing the export licences, State B apparently concluded that the exports would not contribute to destabilizing accumulations. Thus, even as the WA's requirements have become binding on State B through its unilateral declaration, State B did not breach any of these international law obligations.

Human rights obligations of State C

International human rights law [\[Collapse\]](#)

International human rights law applies in cyberspace; individuals enjoy the same human rights online as they enjoy offline.^[60] States are therefore bound by their human rights obligations to both respect and ensure human rights in cyberspace. States also bear international responsibility for the violation of human rights obligations that are attributable to them.^[61]

The **source** of these obligations is primarily treaty law. The two key global treaties are the International Covenant on Civil and



Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR);^[62] many of these treaties' provisions, along with the provisions of the Universal Declaration of Human Rights, are regarded as reflective of customary international human rights law, even though there is no universally accepted

codification. Apart from the ICCPR and ICESCR, there exist important regional human rights treaty systems, especially for Europe (European Convention on Human Rights – ECHR)^[63], the European Union (Charter of Fundamental Rights of the European Union – EUCFR),^[64] and America (American Convention on Human Rights – ACHR)^[65], which provide for adjudicatory mechanisms by which individuals can assert their human rights against States and which have generated a considerable amount of case-law as a result.

In order to determine whether a State has breached its human rights obligations, the following steps of analysis should be conducted:

1. Since cyber operations often take place in the cyber infrastructure of multiple States, the issue of **jurisdiction** must be addressed. Each human rights treaty has its own bespoke jurisdictional requirements and scope. In this regard, every State party to the ICCPR has undertaken “to respect and to ensure to all individuals **within its territory and subject to its jurisdiction** the rights recognized in the [ICCPR]”.^[66]

The UN Human Rights Committee has understood this provision to mean that the human rights obligations recognized within the ICCPR apply not only to persons physically located within a State's territory, but also to situations where the State exercises “power or effective control” either over the territory on which an individual is located (the spatial




















model of jurisdiction) or over the individual (the personal model of jurisdiction).^[67] The International Court of Justice (ICJ) has gone even further by stating that the ICCPR “is applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory”.^[68] A few States (such as the US and Israel) have adopted the contrary view and maintain that human rights obligations do not apply extraterritorially. To date, however, these States remain in the minority.^[69] As such, although the exact criteria for the applicability of human rights obligations to extraterritorial activities of States are not settled and are subject to ongoing academic and political debate,^[70] the prevailing opinion at present is that human rights obligations do apply to some acts of a State outside its territory.

2. If an international human rights regime is applicable, the second question is whether a cyber operation attributable to a State constitutes an **interference** with a particular human right. The human rights that are often implicated by cyber operations include the right to privacy^[71] and the right to freedom of opinion and expression.^[72]

3. Not every State interference with a human right is also a violation of international human rights law. For an interference to be legal, it must be justified, namely:

- a. in accordance with an accessible and foreseeable domestic law (“**legality**”),
- b. pursuing a **legitimate objective** of public interest (such as national security, public order, public health, or morals) or for the protection of rights of others,
- c. **necessary** to achieve that objective, and
- d. **proportionate** in balancing the means and the end.^[73]

Apart from the responsibility for human rights violations attributed to it, a State can also be held responsible for its failure to take all reasonable measures to protect the human rights of individuals in its territory and subject to its jurisdiction (for instance, if it unlawfully allows non-State actors to violate human rights).^[74]

Publicly available national positions that address this issue include:  (2020),  (2022),  (2020),  (2021),  (2020),  (2021),  (2021),  (2021),  (2021),  (2019),  (2020),  (2021),  (2021),  (2022),  (2021),  (2021),  (2012),  (2016),  (2021).

[L14] State C's law enforcement and security agencies used the tool domestically against human rights defenders, lawyers, journalists, activists, opposition politicians, and dissidents. By intruding into their devices, accessing their data, and monitoring them, State C interfered with their right to privacy and freedom of opinion and expression.^[75] Whereas any interference can, in theory, be justified, it is doubtful that the conduct of State C satisfied the necessity and proportionality requirements under the given circumstances.^[76] This is particularly the case taking into account the broad range of categories of people who were subjected to these measures and the apparent absence of any safeguards against abuses of the intercepted information.^[77]

Human rights obligations of State A and B

[L15] States A and B issued export licences to the respective companies for the export of the intrusion tools and related items to State C. The "action" of issuing an export licence did not breach any negative human rights obligations. Only State C's conduct did, which is not attributable to States A and B (see section 2.1 above).

[L16] However, the conduct of a State leading to an internationally wrongful act can consist of an action or an omission.^[78] A failure of States A and B to comply with their positive human rights obligations would be a relevant omission.^[79]

[L17] Part of the positive human rights obligations is arguably the due diligence obligation to not knowingly allow acts contrary to international human rights, whereby constructive knowledge suffices. It is, thus, similar to the due diligence obligation in general international law as employed in the cyber context.^[80] Therefore, the same cumulative elements should be applied, however, only with respect to individuals' human rights. Consequently, States A and B would potentially violate their human rights due diligence obligation if they did not put in place a sufficient export control framework, although they knew or should have known of the general risk to human rights associated with the export of such tools; or if they issued export licences, although they knew or should have known that State C would use the tools in breach of its human rights obligations.

[L18] However, it is debatable whether human rights due diligence obligations are exclusively applicable if an individual is in a State's territory and subject to its jurisdiction; and, if so, whether "jurisdiction" can be construed to include situations of extraterritorial harm. Either way, it can be argued that extraterritorial human rights due diligence obligations exist.^[81]

[L19] In any case, States A and B did not breach their human rights due diligence obligations. There is no indication that States A or B were aware of any human rights violations perpetrated by State C at the time of issuing the licences. Furthermore, there is no indication that they should have known of such violations. States A and B had

incorporated the WA into their domestic law and policies. Consequently, their export control agencies had to assess an importing State's human rights record in the licensing process as part of preventing destabilizing accumulations.^[82] There is no indication that the agencies failed to do so sufficiently in the present case. On the contrary, they immediately revoked all licences after becoming aware of the relevant facts. Therefore, States A and B did not breach their human rights due diligence obligations.

Checklist

- Attribution:
 - Is the “export control agency” a State organ?
 - Did the State aid or assist another State's internationally wrongful act, such as human rights violations, by licensing an export of a cyber tool?
 - What kind of conduct by private companies, thus, non-state actors, can be attributed to States?
- International export control law:
 - Is the State a participating State in the Wassenaar Arrangement (WA)?
 - Is the item in question listed either on the Dual-Use List or the Munitions List of the WA?
 - If the item is listed, did the State apply export controls?
 - What is the consequence of being in non-compliance with the non-binding WA?
 - Did the State declare to follow the WA unilaterally?
 - Is the declaration legally binding or merely political?
- International human rights law and Due diligence:
 - Does the State have an obligation not to knowingly allow companies situated in its territory to export malicious cyber tools to a State that will use the tool for internationally wrongful acts, such as human rights violations?
 - Is the importing State violating the international human rights of individuals in its territory or abroad using the tools?
 - Did the exporting State have actual or constructive knowledge that the importing State would use the intrusion

tool contrary to the rights of and resulting in serious adverse consequences for the human rights of individuals?

- Did the exporting State take all feasible measures to prevent misuse of the intrusion tool?

Appendixes

See also

- [Scenario 07: Leak of State-developed hacking tools](#)
- [Scenario 11: Sale of surveillance tools in defiance of international sanctions](#)
- [Due diligence](#)
- [Attribution](#)
- [Breach of an international obligation](#)
- [Due diligence](#)
- [Voluntary, non-binding norms of responsible state behavior](#)
- [Peacetime cyber espionage](#)
- [International human rights law](#)

Notes and references

1. ILC [Articles on State Responsibility](http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf) (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 4(1).
2. ILC [Articles on State Responsibility](http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf) (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 6.
3. ILC [Articles on State Responsibility](http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf) (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 5.
4. ILC [Articles on State Responsibility](http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf) (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 7; Tallinn Manual 2.0 (<https://doi.org/10.1017/9781316822524>), commentary to rule 15, paras. 6-7 and 12.
5. See in detail Christian Dominicé, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in James Crawford and others (eds), *The Law of International Responsibility* (OUP 2010) 282-284.

6. James Crawford, *State Responsibility: The General Part* (CUP 2013) 333; ILC Articles on State Responsibility, commentary to Part IV, para 1.
7. James Crawford, *State Responsibility: The General Part* (CUP 2013) 336.
8. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art. 16. This concept was applied by the ICJ in the *Bosnian Genocide Case*, see *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgement (2007) para 420.
9. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art. 17. This form of indirect responsibility is rather rare, belligerent occupation being one of the few possible examples. Distinction must be made from the situation where an organ of one State has been placed at the disposal of another State - upon certain conditions, acts of this organ might be attributable to the latter State. See Tallinn Manual 2.0 (<https://doi.org/10.1017/9781316822524>), Rule 16.
10. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art. 18.
11. Christian Dominicé, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in James Crawford and others (eds), *The Law of International Responsibility* (OUP 2010) 284.
12. In situations where aid or assistance is an essential and integral element of the assisted State's operation, assisting State may be responsible for the assisted conduct. Responsibility of the assisting State therefore attaches for the extent of its contribution. See Tallinn Manual 2.0 (<https://doi.org/10.1017/9781316822524>), commentary to Rule 18, para 6.
13. Christian Dominicé, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in James Crawford and others (eds), *The Law of International Responsibility* (OUP 2010) 285; ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), commentary to Art. 16, para 10.

14. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), commentary to Art. 17, para 1, commentary to Art. 18, paras 1 and 7; Tallinn Manual 2.0 (<https://doi.org/10.1017/9781316822524>), commentary to Rule 18, para 6.
15. Christian Dominicé, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in James Crawford and others (eds), *The Law of International Responsibility* (OUP 2010) 288.
16. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), commentary to Art. 23, para 3.
17. Christian Dominicé, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in James Crawford and others (eds), *The Law of International Responsibility* (OUP 2010) 288-289.
18. ARSIWA Commentary to art 16, paras 3–4; Bosnian Genocide (n 8) [432].
19. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 8; see also Kubo Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (<https://doi.org/10.1093/jcs/krw014>) (2016) 21 JC&SL 405.
20. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 9.
21. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 10(1).
22. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 10(2).
23. ILC Articles on State Responsibility (http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf), Art 11.
24. See Mačák (n 19); ARSIWA commentary to art 8, para 3-9.
25. ARSIWA art 5.

26. For example, the Treaty on the Non-Proliferation of Nuclear Weapons (adopted 1 July 1968, entered into force 5 March 1970) 729 UNTS 161 (NPT); Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (adopted 10 April 1972, entered into force 26 March 1975) 1015 UNTS 163 (CBTW); Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997) 1974 UNTS 45 (CWC); Arms Trade Treaty (adopted 2 April 2013, entered into force 24 December 2014) 3031 UNTS 269 (ATT); Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137 (CCW).

27. Especially United Nations Security Council (UNSC), 'Resolution 1540' (28 April 2004) UN Doc S/Res/1540.

28. These are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom and United States, see The Wassenaar Arrangement, 'About us' (<https://www.wassenaar.org/about-us/>) (23.12.2021) .

29. For example, Israel, Taiwan, and the United Arab Emirates.

30. 'Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies' Guidelines & Procedures, including the Initial Elements (12 July 1996) WA-DOC (19) PUB 007 para I.1.

31. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: List of Dual-Use Goods and Technologies (reflects the agreements recorded in Appendix 5 to the Initial Elements, dated 19 December 1995, and all subsequent amendments, including those approved by the Plenary in December 2021) WA-LIST (20) 1 (WA Dual-Use List) and Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Munitions List (reflects the agreements recorded in Appendix 5 to the Initial Elements, dated 19 December 1995, and all subsequent amendments, including those approved by the Plenary in December 2021) WA-LIST (20) 1 (WA Munitions List). The Dual-Use List deals with items that can have both a military and civilian application, and the Munitions List deals with purely military items.

32. Whether those cyber tools qualify as weapons under IHL is controversial; see Legal review of cyber weapons, means and methods of warfare.

33. WA Munitions List ML21.b.5.; does not apply to “vulnerability disclosure” or to “cyber incident response”, limited to non-military defensive cybersecurity readiness or response, see WA Munitions List note 2 to ML21.b.5.; see also the general software note to the WA Munitions List.

34. This “includes ‘software’ designed to destroy, damage, degrade or disrupt systems, equipment or ‘software’, specified by the Munitions List, cyber reconnaissance and cyber command and control ‘software’, therefore.” See WA Munitions List note 1 to ML21.b.5.

35. Which includes the technology required for developing, producing, operating, installing, maintaining (checking) and repairing military offensive cyber tools, see WA Munitions List ML22.a. The WA defines technology as “specific information necessary for the ‘development’, ‘production’ or ‘use’ of a product. The information takes the form of ‘technical data’ or ‘technical assistance’”, see Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Definitions of Terms (reflects the agreements recorded in Appendix 5 to the Initial Elements, dated 19 December 1995, and all subsequent amendments, including those approved by the Plenary in December 2021) WA-LIST (20) 1 (WA Definitions), 234. “‘Technical data’ may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories”, see WA Definitions 234. “‘Technical assistance’ may take forms such as instruction, skills, training, working knowledge, consulting services. ‘Technical assistance’ may involve transfer of ‘technical data’”, see WA Definitions 234.

36. The WA defines intrusion software as “[s]oftware’ specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network-capable device” and to perform either “extraction of data” or “modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions”, see WA Definitions 224.

37. WA Dual-Use List cat 4.A.5. and cat. 4.D.4. Moreover, the list names technology for the “development”, “production” or “use” of intrusion tools, see WA Dual-Use List cat 4.E.1.a. See also the general technology note to the WA Dual-Use List and above n 36. Does not apply to “vulnerability disclosure” or “cyber incident response”, see WA Dual-Use List note 1 to cat 4.E.1.a.

38. 'Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies' Compendium of Best Practice Documents (<https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-005-Public-Docs-Vol-III-Comp.-of-Best-Practice-Documents-Dec.-2019.pdf>) (December 2019) WA-DOC (19) PUB 005.

39. Wassenaar Arrangement, 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons' Explanatory Note (<https://www.wassenaar.org/app/uploads/2019/consolidated/Elements-for-Objective-Analysis.pdf>) (As adopted in 1998 and amended by the Plenary in 2004 and 2011).

40. See *ibid* 1.e, 3.a; Wassenaar Arrangement, 'Best Practice Guidelines for Exports of Small Arms and Light Weapons (SALW)' (<https://www.wassenaar.org/app/uploads/2019/12/Best-practice-guidelines-on-export-of-SALW-web-version.pdf>) (2002) (Agreed at the 2002 Plenary and amended at the 2007 and 2019 Plenary) 1–2 ; moreover, items related to intrusion tools were added by the participating States due to the human rights concerns associated with such tools, E Korzak, 'Export Controls: The Wassenaar experience and its lessons for international regulation of cyber tools' in E Tikk and M Kerttunen (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020) 305; but see also UN Human Rights Council, 'Surveillance and human rights' Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (28 May 2019) UN Doc A/HRC/41/35 para. 34–38, 66(f) recommending that participating States "should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights."

41. 'Wassenaar Arrangement' 5.

42. UN International Law Commission, Guiding Principles Applicable to Unilateral Declarations of States Capable of Creating Legal Obligations, with Commentaries thereto (adopted at its Fifty-eighth session, in 2006) UN Doc A/CN.4/SER.A2006/Add.1 (Part 2) (ILC Guiding Principles), principle 2; Nuclear Test Case (Australia v. France) [1974] ICJ Rep 253, [43]. Examples are the public statements of the French President and Foreign and Defence Ministers to cease nuclear tests in the South Pacific, see Nuclear Test Case (New Zealand v. France) [1974] ICJ Rep 457, [43–50]; Egypt's 1957 Declaration on the Suez Canal; Jordan's 1988 waiver of claims to the West Bank; U.S. representations before the WTO Dispute Settlement Body in the 1974 Trade Act case; and (at least potentially) US and Soviet 1977 declarations in relation to the Strategic Arms Limitation Talks; and Cuba's 2002 declarations about the supply of vaccines to Uruguay.

43. ILC Guiding Principles principle 1; Nuclear Test Case (Australia v France) (n 43) [46]; Nuclear Test Case (New Zealand v France) (n 43) [49].

44. K Ziolkowski, 'Confidence Building Measures for Cyberspace – Legal Implications' (<https://ccdcoe.org/uploads/2018/10/CBMs.pdf>) (2013) 23–24 .

45. PC Anderson, 'Cyber Attack Exception to the Foreign Sovereign Immunities Act' (<https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4729&context=clr>) (2017) 102(4) Cornell Law Review 1087, 1109 .

46. See for an overview of available position papers the section National positions .

47. ILC Guiding Principles principle 1; Nuclear Test Case (Australia v France) (n 43) [43]; VR Cedeño and MIT Cazorla, 'Unilateral Acts of States in International Law' in A Peters (ed), Max Planck Encyclopedias of International Law (OUP) para 19.

48. ILC Guiding Principles principle 5.

49. ILC Guiding Principles principle 6.

50. ILC Guiding Principles principle 1; Nuclear Test Case (Australia v France) (n 43) [43].

51. ILC Guiding Principles principle 3.

52. ILC Guiding Principles principle 4.

53. ILC Guiding Principles principle 4.

54. ILC Guiding Principles principle 7; Nuclear Test Case (Australia v France) (n 43) [43, 51]; Nuclear Test Case (New Zealand v France) (n 43) [46, 53]; Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) [2005] ICJ Rep 168, [50, 52].

55. ILC Guiding Principles principle 7.

56. ILC Guiding Principles principle 7; Nuclear Test Case (Australia v France) (n 43) [44, 47]; Anglo-Iranian Oil Co (United Kingdom v Iran) (Preliminary Objection) [1952] ICJ Rep 93, [106–108].

57. See also the proposal by B Müller, W Geldhof and T Ruys, ‘Unilateral Declarations: The Missing Legal Link in the Bali Action Plan’ (May 2010) (<https://www.law.kuleuven.be/iir/nl/onderzoek/opinies/ecbiUDsfinal.pdf>) to use binding unilateral declarations to “transform” non-binding GOP decisions in the context of greenhouse gas emission reductions into binding international law.

58. See WA Dual-Use List cat 4.A.5, 4.D.4, and 4.E.1.a.; see also above n 38.

59. ‘Wassenaar Arrangement’ 5.

60. See, for example, United Nations Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, Resolution A/HRC/RES/32/13 (<https://digitallibrary.un.org/record/845728?ln=en>) (1 July 2016), para 1; NATO, *Warsaw Summit Communiqué* (https://www.nato.int/cps/en/natohq/official_texts_133169.htm) (9 July 2016), para 70; *G8 Summit of Deauville, Declaration: Renewed Commitment for Freedom and Democracy* (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf) (27 May 2011), para II/11.

61. See, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Judgment) [2007] ICJ Rep 43 (<https://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-00-EN.pdf>), para 170.

62. International Covenant on Civil and Political Rights (adopted 16 December 1966 (<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>), entered into force 23 March 1976) 999 UNTS 171 (ICCPR); International Covenant on Economic, Social and Cultural Rights (<https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx>) (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).
63. Formal title: Convention for the Protection of Human Rights and Fundamental Freedoms (https://www.echr.coe.int/Documents/Convention_ENG.pdf) (opened to the signature in Rome on 4 November 1950, entered into force 3 September 1953), ETS 5 (ECHR); there are several protocols which significantly expand and amend the obligations of the original Convention.
64. Charter of Fundamental Rights of the European Union (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>), proclaimed on 7 December 2000 (EUCFR).
65. American Convention on Human Rights (<https://doi.org/10.1017/9781316577226.029>) (open for signature from 22 November 1969, entered into force 18 July 1978), 1144 UNTS 123 (ACHR).
66. Article 2(1) ICCPR (<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>).
67. UN HRC, 'General Comment No. 31 (80): The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (<http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2bfud3cPVrcM9YR0iW6Txaxgp3f9kUFpWoq%2fW%2fTpKi2tPhZsbEJw%2fGeZRASjdFuuJQRnbJEaUhby31WiQPI2mLFDe6ZSwMMvmQGVHA%3d%3d>)' (adopted on 29 March 2004, 2187th meeting), para 10.
68. Cf, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* (Advisory Opinion) [2004] (<https://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf>) ICJ Rep 136, para 111.

69. See, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories (Advisory Opinion) [2004] (<https://www.icj-cij.org/files/case-related/131/131-20040709-ADV-01-00-EN.pdf>) ICJ 136, para 110; UN HRC, *Summary Record of the 1405th Meeting*, CCPR/C/SR.1405 (31 March 1995) 6 [20].

70. See, for example, Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (<https://www.ilsa.org/Jessup/Jessup16/Batch%202/MilanovicPrivacy.pdf>) (2015) 56 Harvard International Law Journal 81.

71. Article 17 ICCPR (<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>); Article 8 ECHR (https://www.echr.coe.int/Documents/Convention_ENG.pdf); Article 7 EUCFR (http://www.europarl.europa.eu/charter/pdf/text_en.pdf); Article 11 ACHR (https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf). The exact titles and scopes of the provisions vary.

72. Article 19 ICCPR (<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>); Article 10 ECHR (https://www.echr.coe.int/Documents/Convention_ENG.pdf); Article 11 EUCFR (http://www.europarl.europa.eu/charter/pdf/text_en.pdf); Article 13 ACHR (https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf). The exact titles and scopes of the provisions vary.

73. UN Human Rights Committee, ICCPR General Comment No. 34 (<https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>) (12 September 2011), paras 21-36; See also ICCPR General Comment No. 27 (https://www.nichibenren.or.jp/library/ja/kokusa_i/humanrights_library/treaty/data/HRC_GC_27e.pdf) (1 November 1999), paras 14-16.

74. See, Velásquez Rodríguez v. Honduras (http://hrlibrary.umn.edu/iachr/b_11_12d.htm), (Merits) IACrHR (Ser. C) No. 4 (29 July 1988) [177].

75. ICCPR arts 17 and 19.

76. See also Scenario 11: Sale of surveillance tools in defiance of international sanctions.

77. See ECtHR, *Roman Zakharov v. Russia* (App no 47143/06) (2015) (Grand Chamber Judgment), paras 227–236; ECtHR, *Big Brother Watch and Others v. the United Kingdom* (App nos 58170/13, 62322/14 and 24960/15) (Grand Chamber Judgment), paras 332–339; ECtHR, *Centrum för Rättvisa v. Sweden* (App no 35252/08) (2021) (Grand Chamber Judgment), paras 246–253; UN Human Rights Committee, Concluding Observations on The Netherlands (25 August 2009) UN Doc CCPR/C/NLD/CO/4 para 14; UN Human Rights Committee, Concluding Observations on Sweden (2 April 2009) UN Doc CCPR/C/SWE/CO/6 para 18; UN Human Rights Committee, Concluding Observations on Zimbabwe (6 April 1998) UN Doc CCPR/C/79/Add.89 para 25.

78. ARSIWA art 2.

79. ARSIWA commentary to art 2, para 9 (“Whether a particular obligation is breached forthwith upon a failure to act on the part of the responsible State, or whether some further event must occur, depends on the content and interpretation of the primary obligation and cannot be determined in the abstract.”); ARSIWA commentary to art 4, para 5 (“The principle of the unity of the State entails that the acts or omissions of all its organs should be regarded as acts or omissions of the State for the purposes of international responsibility.”).

80. See Due diligence; on the concept of due diligence in general see H Krieger, A Peters and L Kreuzer (eds), *Due Diligence in the International Legal Order* (OUP 2020); T Koivurova, ‘Due Diligence’ in A Peters (ed) (n 48); A Ollino, *Due Diligence Obligations in International Law* (CUP 2022).

Arguably, a State’s obligation to control the export of intrusion tools and related items cannot only be based on human rights due diligence but on the concept as a whole.

81. See S Besson, 'Due Diligence and Extraterritorial Human Rights Obligations - Mind the Gap!' (2020) 9(1) ESIL Reflections 1; M Monnheimer, *Due Diligence Obligations in International Human Rights Law* (CUP 2021) 258–321; F Violi, 'The function of the triad 'territory', 'jurisdiction', and 'control' in due diligence obligations' in H Krieger, A Peters and L Kreuzer (eds) (n 80) 81–82; VP Tzevelekos, 'Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' (2014) 36(1) *Michigan Journal of International Law* 129; but see M Brehm, 'The Arms Trade and States' Duty to Ensure Respect for Humanitarian and Human Rights Law' (2007) 12(3) *Journal of Conflict and Security Law* 359, 380–383; A Ollino (n 80) 149–156. See also in that direction 'Guiding Principles on Business and Human Rights' Implementing the United Nations 'Protect, Respect and Remedy' Framework (2011) UN Doc HR/PUB/11/04, principles 1-3, 7.

82. A human rights risk assessment is specifically mentioned within the Wassenaar Arrangement concerning conventional weapons and small arms and light weapons, see Wassenaar Arrangement, 'Elements' (n 40) 1.e; Wassenaar Arrangement, 'Best Practice SALW' (n 41) 1–2; Moreover, items related to intrusion tools were added by the participating States due to the human rights concerns associated with such tools, see Korzak (n 41) 305.

Bibliography and further reading

- Baade B, 'Due Diligence and the Duty to Protect Human Rights' in H Krieger, A Peters and L Kreuzer (eds), *Due Diligence in the International Legal Order* (OUP 2020).
- Besson S, 'Due Diligence and Extraterritorial Human Rights Obligations - Mind the Gap!' (2020) 9(1) ESIL Reflections 1.
- Brehm M, 'The Arms Trade and States' Duty to Ensure Respect for Humanitarian and Human Rights Law' (2007) 12(3) *Journal of Conflict and Security Law* 359.
- Bromley M and Maletta G, 'The Challenge of Software and Technology Transfers to Non-proliferation Efforts: Implementing and Complying with Export Controls' (Stockholm April 2018)

<https://www.sipri.org/publications/2018/other-publications/challenge-software-and-technology-transfers-non-proliferation-efforts-implementing-and-complying> accessed 14 February 2020.

- Bruin E de, 'Export Control Regimes—Present-Day Challenges and Opportunities' in R Beeres and others (eds), NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade (T.M.C. Asser Press; Springer 2021).
- Cedeño VR and Cazorla MIT, 'Unilateral Acts of States in International Law' in A Peters (ed), Max Planck Encyclopedias of International Law (OUP Online).
- Chircop L, 'A Due Diligence Standard of Attribution in Cyberspace' (2018) 67(3) International and Comparative Law Quarterly 643.
- Crawford J, State Responsibility: The General Part (CUP 2013).
- Dominicé C, 'Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State' in J Crawford, A Pellet and S Olleson (eds), The Law of International Responsibility (OUP 2010).
- Dörr O, 'Declaration' in A Peters (ed), Max Planck Encyclopedias of International Law (OUP Online).
- Fidler M, 'Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities' (Dissertation, Stanford University Mai 2014).
- Joyner DH (ed), Non-proliferation export controls: Origins, challenges, and proposals for strengthening (Ashgate 2006).
- Kanetake M, 'Controlling the Export of Digital and Emerging Technologies: Security and Human Rights Perspectives' (2021) 31(1-4) Security and Human Rights 1.
- Kim H, 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue' (2021) 70(2) International and Comparative Law Quarterly 379.
- Klein R, 'Trimming Pegasus' Wings: International Export Control Law and 'Cyberweapons' (27 October 2021) <https://voelkerrechtsblog.org/trimming-pegasus-wings/> accessed 10 January 2022.

- Koivurova T, 'Due Diligence' in A Peters (ed), Max Planck Encyclopedias of International Law (OUP Online).
- Korzak E, 'Export Controls: The Wassenaar experience and its lessons for international regulation of cyber tools' in E Tikk and M Kerttunen (eds), Routledge Handbook of International Cybersecurity (Routledge 2020).
- Krieger H, Peters A and Kreuzer L (eds), Due Diligence in the International Legal Order (OUP 2020).
- Lin H and Trachtman J, 'Diagonal Export Controls to Counter Diagonal Transnational Attacks on Civil Society' (2020) 31(3) European Journal of International Law 917.
- Mačák K, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21(3) Journal of Conflict and Security Law 405.
- Marauhn T, 'Global governance of dual-use trade: the contribution of international law' in O Meier (ed), Technology Transfers and Non-Proliferation: Between control and cooperation (Routledge 2013).
- Monnheimer M, Due Diligence Obligations in International Human Rights Law (CUP 2021).
- Mulbry E, 'Arms Control 2.0: Updating the Cyberweapon Arms Control Framework' (2021) 28(1) Michigan Technology Law Review 175.
- Schmitt MN (ed), Tallinn manual 2.0 on the international law applicable to cyber operations (CUP 2017).
- Ollino A, Due Diligence Obligations in International Law (CUP 2022).
- Tamada D and Achilleas P (eds), Theory and Practice of Export Control: Balancing International Security and International Economic Relations (Springer 2017).
- Tzevelekos VP, 'Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' (2014) 36(1) Michigan Journal of International Law 129.
- Violi F, 'The function of the triad 'territory', 'jurisdiction', and 'control' in due diligence obligations' in H Krieger, A Peters and

L Kreuzer (eds), *Due Diligence in the International Legal Order* (OUP 2020).

- Voetelink J, 'International Export Control Law—Mapping the Field' in R Beeres and others (eds), *NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade* (T.M.C. Asser Press; Springer 2021).
- Wolfrum R, 'Obligation of Result Versus Obligation of Conduct: Some Thoughts About the Implementation of International Obligations' in MH Arsanjani and others (eds), *Looking to the Future: Essays on International Law in Honor of W. Michael Reisman* (Brill 2010).

Contributions

- Scenario by: [Roland Klein](#)
- Analysis by: [Roland Klein](#)
- Reviewed by: [Marjolein Busstra](#), [François Delerue](#) and [Asaf Lubin](#)

Previous: [Scenario 25: Cyber disruption of humanitarian assistance](#)

Next: [Scenario 27: Contesting and redirecting ongoing attacks](#)

Retrieved from "https://cyberlaw.ccdcoe.org/w/index.php?title=Scenario_26:_Export_licensing_of_intrusion_tools&oldid=3572"

This page was last edited on 15 October 2022, at 14:53.

Content is available under Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) unless otherwise noted.