Challenging State-Sponsored Economic Espionage under International Law

This report elaborates on how to assess state-sponsored economic espionage (hereafter economic espionage) under international law, and describes the difficulties for a state to challenge another state on legal grounds for having engaged in economic espionage. The current state of play leaves economic espionage relatively unregulated, which may explain why governments resort to other measures of unilateral nature instead, such as economic sanctions, or negotiating political commitments from states accused of engaging in economic espionage.

This report first reviews the term 'economic espionage', and thereafter provides an overview of how, if at all, economic espionage could be challenged under international law and international trade law rules under the WTO. The report then further describes how states use economic sanctions and bilateral – political – negotiations to try to prevent economic espionage.
Economic espionage

COMMON USE OF THE TERM

ECONOMIC ESPIONAGE

Economic espionage (also referred to as commercial espionage) is a relatively new but legally undefined term. It is commonly used to identify espionage by a state actor against a private commercial operator (company) in another country. The purpose of economic espionage is to collect and obtain business confidential information relating to foreign companies and to relay such information to domestic companies. The collection of information (the espionage) is done by a state agency or state-affiliated proxy, however the purpose is to transfer the information acquired through espionage for the purpose of promoting domestic companies. Thus, the espionage is driven and characterised by an economic interest, in contrast to traditional forms of espionage, which are driven by national security or defence interest. Information typically pursued is business confidential information such as customer data, contract information, operational information such as production and logistical data, as well as other trade secrets.

Broken down to its basics, economic espionage is not a legitimate form of business. It is rather a hybrid between (as explained below) unregulated espionage conducted by a state and theft of trade secrets, which in most cases is illegal under domestic laws (a criminal act or an act that at least carries civil liability).

Over the past years, the number of reports of cyber-enabled economic espionage has escalated. This may be a reflection of the fact that economies and industries have become more digitally connected on a global scale and therefore also face an increasing exposure to economic espionage through cyberspace.

ECONOMIC ESPIONAGE IS A FORM OF CYBER ESPIONAGE

Economic espionage is increasingly carried out in cyberspace, i.e. a form of cyber espionage. Furthermore, the culprit of economic espionage is usually a state agency or a proxy of the state. It is therefore relevant to start the analysis by reviewing how international law regulates state responsibility for cyber espionage. In this respect, the Tallinn Manual 2.0 on the International Law Applicable

---

1 See for example the U.S. Federal Bureau of Investigation’s definition: https://www.fbi.gov/about/faqs/what-is-economic-espionage.


to Cyber Operations (the “Manual”), is a useful tool for assessing a state’s responsibility vis-à-vis other states or private companies in other countries.

The Manual defines cyber espionage as an act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. This definition includes capabilities to monitor, capture or exfoliate electronically transmitted or stored communication, data, or other information.

If the economic espionage is carried out by the state against its own nationals (legal or natural persons) such actions could trigger the domestic laws of that state, which will govern the relationship between the state and its subjects. When the violation of intellectual property rights or theft of trade secrets is done by a company against another, this is also usually handled under domestic laws. However, when a state is spying and stealing trade secrets of a company in another state, the actions transcend domestic law and pass into the realm of international law.

The Manual analyses various types of cyber operations by a state, and provides guidance under international law as to when acts should be considered lawful or unlawful. Only if deemed unlawful, would the action trigger state responsibility under international law.

**Lawful and unlawful espionage under international law**

The principle of state sovereignty, which is a fundamental legal principle under international law, establishes that a state rules over its own territory, both internally by regulating and protecting its territory and subjects (e.g. natural and legal persons), and externally, i.e. that other states must respect its territorial boundaries. States may thus not engage in unlawful breaches of the principle of sovereignty or intervention (as defined below) against another state. If it does, the former may take countermeasures. These principles apply equally in cyberspace.

---

4 The Tallinn Manual was commissioned by NATO’s Co-Operative Cyber Defence Centre of Excellence to apply existing international law to cyber-related issues, providing an expert-led policymaking reference tool on cyber security.

5 State responsibility under international law is not regulated through any convention or treaty. The International Law Commission’s Article of State Responsibility have been commended by the UN General Assembly, but have not entered into force. Nonetheless, these provisions are frequently cited in courts and tribunals, see page 79 of the Manual.

ECONOMIC ESPIONAGE

LAWFULNESS OF CYBER ESPIONAGE
The Manual concludes that customary international law does not prohibit cyber espionage per se.7 Cyber espionage, including economic espionage, as such, is therefore not unlawful under international law.8 Some scholars have however argued that economic espionage should be treated differently, in that economic espionage violates the economic sovereignty of a state.9

However, if the espionage (including economic espionage), is undertaken in ways that would violate other customary international laws, such as the principle of sovereignty or the principle of non-intervention, the espionage could be deemed unlawful.10

Thus, an important distinction has to be made between a state’s cyber operations which constitute lawful cyber espionage, on the one hand, and other acts which violate obligations of international law, such as the principles of sovereignty or non-intervention, on the other. Accordingly, the latter would trigger state responsibility allowing the other state to take countermeasures.

For example, if the espionage is undertaken with the purpose of intervening in internal affairs or political elections, such espionage would violate customary international law.11 Equally, other forms of cyber activities by a state such as attacks on another state’s availability or integrity of critical infrastructure could be classified as a breach of the principle of internal sovereignty. Furthermore, a state’s internal sovereignty encompasses its cyber infrastructure, regardless of if it is run or owned by the government or by private operators.12 Thus, an intervention against a privately run public network, could be seen as unlawful and trigger state responsibility even if the activity has no effect on any government cyber infrastructure, assets, or activities.13

Thus, to be considered unlawful, the economic espionage would have to breach, for example, the principle of sovereignty or principle of non-intervention. Simply stealing business confidential information and relaying such information to a domestic company, would likely not be considered unlawful under international law.

PRINCIPLE OF DUE DILIGENCE
The principle of sovereignty expands into the principle of due diligence, which in short means that states are obliged to not allow, knowingly, its territory to be used for acts contrary to the rights of other states.14 Put differently, a state must, within its territory, indirectly protect the rights of other states. For example, if a state knows that another state is using servers in its territory to commit unlawful espionage against a third state, the first state is obliged to protect the rights of the third state.15

Again however, the due diligence principle applies only in respect of internationally wrongful (unlawful) acts.16 As cyber espionage, and therefore also economic espionage, is not per se unlawful under customary international law,17 there is also no obligation to prevent economic espionage unless, as discussed above, it would constitute a violation of the principles of sovereignty or non-intervention.

---

7 See page 168 of the Manual.
8 See pages 169–172 of the Manual. In particular, note 386 explains the view that a state may bilaterally commit to refraining from economic espionage, taking as an example the U.S. and China commitments in 2015 (see also section 6 of this report).
10 See page 170 of the Manual “For instance, if organs of one State, in order to extract data, back into the cyber infrastructure located in another State in a manner that results in a loss of functionality, the cyber espionage operation violates, in the view of the Experts, the sovereignty of the latter. Similarly, if cyber operations that are undertaken for espionage purposes violate the international human right to privacy (Rule 35), the cyber espionage operation is unlawful.”
12 Id. pages 13–14.
13 Id. page 18.
14 Id. page 30.
15 Id. page 34.
16 Id. page 34.
17 Id. page 168.
Possible remedies under domestic law or bilateral investment treaties

CHALLENGING A STATE IN A DOMESTIC COURT
A company that has suffered from economic espionage could try to bring an action for damages in a domestic court proceeding in its own jurisdiction. Many states have enacted domestic laws prohibiting theft of trade secrets, which apply equally to thefts through cyberspace, which presumably apply even if committed by a state. Examples of such laws are the Economic Espionage Act of 1996 in the U.S. and EU Directive 2016/943 on protection of trade secrets, which is further implemented through national laws in various EU Member States.¹⁸

If challenged in a national court of another state, the challenged state would however likely try to invoke the principle of state immunity, under which states enjoy immunity from the jurisdiction of the courts of another state.¹⁹ However state immunity is not an absolute right in all situations. The principle applies to a state’s exercise of its sovereign powers (jure imperii) but not necessarily to a state’s actions relating to non-sovereign activities, such as private or commercial activities (jure gestionis).²⁰

Economic espionage, to the extent it qualifies as a violation of intellectual property rights, should arguably be treated as an act comparable to commercial activities, jure gestionis.²¹ A state would then not be able to claim state immunity for such acts and could thus instead face a normal trial in a domestic court. A company would in any event need to make plausible that a state is responsible for the economic espionage and establish a causal link to damage suffered.

BILATERAL INVESTMENTS TREATIES
Another possible alternative for a company suffering from economic espionage could be to claim a breach of any applicable bilateral investment treaty ("BIT"). Such treaties oblige the contracting states to protect investments made by each other’s nationals in their respective territory.

The company claiming damages under a BIT would have to show that it has an investment in the state that has conducted the economic espionage, and that its investment has suffered damage from the economic espionage. It could then be argued that, by stealing trade secrets, the state has failed to protect the investment as required by the BIT. As with the WTO agreements (as described below), the claiming party would need to also establish a causal link between the espionage occurring in another country and a damage suffered by the investment in the contracting state. If however the economic espionage is carried out at the local level and results in the deprivation of the value of the investment, the case would be more clear and comparable to typical expropriation in a BIT challenge.

---

¹⁸ Economic espionage would likely be categorised as a criminal act under the domestic laws of the countries that implement the Budapest Convention on Cybercrime (Council of Europe, Treaty no. 185). The Budapest Convention focuses on law-enforcement and sanctions due to cybercrime, rather than measures to prevent such cybercrime.

¹⁹ The principle of state immunity is derived from customary international law, and in particular the principle of sovereignty (see, e.g. para. 54 of the International Court of Justice judgement Jurisdictional Immunities of the State, 3 February 2012). The United Nations has tried to codify this principle in the Convention on Jurisdictional Immunities of States and Their Property, which was adopted by the General Assembly on 2 December 2004 but has not yet entered into force (the "Convention").

²⁰ See para. 60 of the International Court of Justice judgement Jurisdictional Immunities of the State, of 3 February 2012.

²¹ For reference, the Convention lists actions which do not benefit from state immunity. Article 14 of the Convention states that a state cannot invoke immunity from jurisdictions before a court of another State which is otherwise competent in a proceeding which relates to... (b) an alleged infringement by the State, in the territory of the State of the forum, of a right of the nature mentioned in subparagraph (a) [a patent, industrial design, trade name or business name, trademark, copyright or any other form of intellectual or industrial property which enjoys measures of legal protection] which belongs to a third person and is protected in the State of the forum.
International trade rules under the WTO

USING THE WTO DISPUTE SETTLEMENT SYSTEM
Besides the international law aspects, some scholars argue that states should try to find recourse against economic espionage by invoking WTO rules and in particular the agreement regarding intellectual property rights (“TRIPS”). As such, the WTO agreements, including the TRIPS-agreement, are multilateral treaties, the purpose of which are to encourage global trade by lowering trade tariffs and barriers and ensuring a more predictable and rule-based trading system. The WTO agreements thereby confer rights and impose obligations related to trade on WTO members, i.e. granting trade preferences (bound import tariffs) and non-discriminatory access to each other’s markets.

The WTO’s enforcement mechanism allows a WTO member (a state) to bring action before the Dispute Settlement Body (“DSB”) against another WTO member for violating the provisions of any of the WTO agreements. If a claimant prevails, the responding state has to restore the rights of the prevailing party, or face the risk of retaliatory measures. A DSB-ruling also has a potentially wider benefit, as it may set a precedent and deter other states from engaging in similar practices.

The critical question is therefore if economic espionage would be seen as a violation of any specific obligations or rights in any of the WTO agreements, in order for the DSB to admit and try a claim. Currently, there is an on-going debate amongst scholars of whether the WTO agreements in fact would be applicable to economic espionage.

Several scholars have pointed out that none of the WTO agreements explicitly obliges a WTO member to refrain from economic espionage. This is understandable, as the WTO agreements are designed to encourage legitimate trade and have not focused on illegitimate trade (theft of trade secrets).

Mounting a WTO case against economic espionage
Several scholars have pointed out that none of the WTO agreements explicitly obliges a WTO member to refrain from economic espionage. This is understandable, as the WTO agreements are designed to encourage legitimate trade and have not focused on illegitimate trade (theft of trade secrets).

24 Established by the Understanding on Rules and Procedures Governing the Settlement of Disputes.
Initial considerations: attribution, laws or practices
A WTO member would first need to ascertain that the economic espionage is a “measure” taken by another member. An apparent difficulty, as with cyber-attacks in general, is attribution, i.e. establishing with certainty who committed the act or on whose behalf the act was committed. An act of economic espionage would thus have to be attributed to a particular state actor. Further, the claim would have to be built on either an “as such” claim, i.e. against a specific law or rule, or an “as applied” claim, against a specific practice. Both claims present difficulties, as economic espionage is usually not mandated by law or regulated openly, and the claimant state would likely have difficulties collecting evidence to show that the acts of espionage constitute a consistent practice. Apart from establishing attribution and the facts, i.e. that another WTO member has collected or stolen business confidential information or trade secrets from a company and transferred such information to a company in its own jurisdiction, the claimant would also need to identify the substantive provisions of the WTO agreements that have been breached.

Identifying WTO rights or obligations violated by economic espionage
Some authors claim that economic espionage could be challenged as a violation of the TRIPS-agreement, in particular Article 39, as well as Article 10bis of the Paris Convention for the Protection of Intellectual Property (the “Paris Convention”) which is incorporated into TRIPS. Article 10bis of the Paris Convention has extensive language and requires a member to provide “effective protection against unfair competition”, which is defined as “any act of competition contrary to honest practices in industrial or commercial matters.” Acts of “unfair competition” could be interpreted narrowly to mean acts in relation to consumers only, and a broader interpretation would be needed to encompass also theft of trade secrets. Even if interpreted broadly, the obligation to prevent economic espionage would usually apply within each state’s territory only. In other words, a state is obliged to ensure protection for companies from other states when operating in its territory. However, that obligation does not necessarily extend to acts committed elsewhere, i.e. when a government spies on companies outside its territory.

Article 39 TRIPS could also be relied on to claim that economic espionage constitutes a violation of WTO law. According to Article 39.2 TRIPS, WTO members have to ensure that natural or legal persons are provided the “possibility of preventing information lawfully in their control from being disclosed to, acquired by, or used by others without their consent”. In other words, an obligation related to non-disclosure of trade secrets. The key question is whether the obligation to provide “possibility of preventing”, also amounts to an obligation to protect against disclosure. A literal interpretation of the wording would suggest that a WTO member is obliged to ensure that there is a legal regime to challenge disclosure of trade secrets in their respective domestic laws only, and that nothing in Article 39.2 TRIPS imposes an outright ban on the government to conduct espionage, or from disclosing information collected through espionage to others. However, interpreting Article 39 TRIPS based on the spirit of the agreement would instead suggest that economic espionage against a foreign company would constitute a violation.

27 Jamie Strawbridge, supra note 23.
29 See Jamie Strawbridge, supra note 23, pages 848–851. See also Stuart S. Malawer, supra note 25, page 4, which highlights that the WTO principle of National Treatment (Article III TRIPS) would apply in particular in such cases.
30 The key question in the legal debate is whether the WTO commitment in TRIPS and the Paris Convention applies outside a WTO member when conducting economic espionage outside its own territory.
31 TRIPS-agreement, supra note 22.
32 See Jamie Strawbridge, supra note 23, page 859.
Besides overcoming this question, as is the case with Article 10bis of the Paris Convention, there is legal uncertainty as to whether Article 39 TRIPS would extend to economic espionage conducted by a government against a foreign company in the company’s home country or in a third country.

Based on the above interpretation, a state could thus live up to its obligation under Article 39 TRIPS by simply providing a domestic legal regime for foreign companies established in their territory to challenge unlawful disclosure of trade secrets, while at the same time spying on the same companies in their home country. Although it seems unreasonable that the drafters of TRIPS had intended for economic espionage to be left completely unregulated, this is likely not an intended mistake but rather the result of digital advancement enabling economic espionage through methods that were not possible to envision at the time.

Economic sanctions

An alternative to a WTO challenge is for a government to unilaterally target another government or individuals by imposing economic sanctions against economic espionage.

Economic sanctions are usually imposed by the United Nations Security Council, but can also be imposed unilaterally by states, for e.g. serious violations of international law or human rights violations. Economic sanctions may take several forms, including designating individuals or companies, and making them subject to an asset freeze and trade ban. Sanctions may also include trade restrictions against certain products or services in a specific country. The use of economic sanctions is per se a disruption of trade between WTO members, and thus in principle also a discriminatory treatment in violation of the trade preferences guaranteed by the WTO agreements. However, most scholars agree that GATT Article XXI, which is a general exemption, gives WTO members the right to impose economic sanctions as a form of measure to protect national security interests. As this provision has very rarely been tested, a key legal question is whether economic espionage, being an economically driven activity, would qualify as a sufficient threat to call for protection of national security interests.

A first example of economic sanctions against economic espionage, is the U.S. program on cyber-related sanctions program managed by the Office of Foreign Asset Control (“OFAC”) which was initiated on 1 April 2015 and further expanded in December 2016, in the wake of the 2016 elections. Accordingly, OFAC may block the property of any person that is responsible for or complicit in cyber-enabled activities that threaten national security, foreign policy or economic health or financial stability of the United States, the purpose or effect of which is, inter alia, “causing a significant misappropriation of funds and economic resources, trade secrets”. In December 2016, the U.S. president listed five entities and four individuals in Russia for their interference with the U.S. government elections. It appears that until now, the U.S. has not yet imposed economic sanctions due to economic espionage (disclosure of trade secrets), although media reports in 2015 suggest that the purpose of the

---

33 The U.S. has discussed the use of “trade tools”, which appears to include trade restrictions, Stuart S. Malawer, supra page 3.
34 See for example David Fuller, supra note 25, and Stuart S. Malawer, supra page 6.
program was to deter China from conducting economic espionage.\textsuperscript{37}

The EU has also considered using economic sanctions as a tool to combat cyber security threats and attacks. In June 2017, the EU Council released its conclusions on the adoption of a Cyber Diplomatic Toolbox, stating that the EU would consider using economic sanctions (restrictive measures) in response to malicious cyber activities.\textsuperscript{38} This was further reiterated in the Council Conclusions of 20 November 2017.\textsuperscript{39} To date, the EU has not yet started using economic sanctions in respect of economic espionage.

### Bilateral political commitments against economic espionage

Economic espionage may, for the time being, be considered unregulated in the international law context or under international treaties, and some states have instead engaged in informal political or diplomatic commitments.

In September 2015, the United States and China made mutual political commitments, pledging not to “conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage”.\textsuperscript{40} This commitment was made shortly after President Obama had issued the cyber-related sanctions program, which may have worked as an incentive for China to agree to U.S. demands.\textsuperscript{41} Whilst commentators have observed a marked decline in detected Chinese cyber-attacks on U.S. companies, there is disagreement as to the role of the agreement in prompting such a decline.\textsuperscript{42}

Other countries, including most of the United States’ partners in the so-called Five Eye intelligence alliance, have followed suit. Great Britain, Russia, Brazil and, Australia\textsuperscript{43} have reportedly all negotiated similar deals with China.\textsuperscript{44} In June 2017, Canada also required China to take on similar commitments in the course of free trade negotiations.\textsuperscript{45} Similar multilateral commitments have also been made in the G-20 in November 2015.\textsuperscript{46}

These political commitments surely carry a strong political message, but are not necessarily legally binding bilateral deals or treaties. The enforceability of the commitments is also questionable. There appears to be no foreseen consequences for breaching these commitments, other than political damage. The option of a bilateral commitment appears relatively weak unless coupled with another instrument, such as the threat of economic sanctions (as shown by the U.S. case).

### Summary

The following table summarises the options reviewed above for challenging economic espionage.

<table>
<thead>
<tr>
<th>Option</th>
<th>Summary of findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>International (customary) law challenge by state</td>
<td>Espionage is per se not unlawful. Other principles, such as sovereignty, would have to be violated</td>
</tr>
<tr>
<td>Domestic court challenge by affected company</td>
<td>Attribution and evidence, claiming non-state immunity</td>
</tr>
<tr>
<td>Bilateral Investment Treaty, by affected company</td>
<td>Company would have to have an investment in the state, and show a link to the failed investment</td>
</tr>
<tr>
<td>WTO (TRIPS) challenge</td>
<td>Uncertain application, due to wording of provisions and geographical limitation of WTO commitments</td>
</tr>
<tr>
<td>Economic sanctions</td>
<td>Possible as a unilateral measure, however requires a form of national security test</td>
</tr>
<tr>
<td>Bilateral commitments</td>
<td>Lack of enforcement of commitments</td>
</tr>
</tbody>
</table>


\textsuperscript{39} Available at: http://www.consilium.europa.eu/media/31666/st14435en17.pdf.


\textsuperscript{44} https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/962910a4-480b-11e5-8ab4-c73967a143cd_story.html?utm_term-b2974bac12d3.

Mannheimer Swartling is the leading commercial law firm in the Nordic region with an international practice and assignments all over the world. By combining the highest legal competence with industry know-how, we offer our clients professional legal advice with added value.