Economic cyber espionage and due diligence

Prof Nicholas Tsagourias

Nicholas.Tsagourias@sheffield.ac.uk

May 2015

Cyber espionage is the clandestine collection of protected information, or of intelligence resident on computers, using cyber means. Economic cyber espionage involves the clandestine collection of trade secrets. Cyber espionage and economic cyber espionage can be state-sponsored -when a government collects information directly or through proxies- but it can also take place between private enterprises. In the latter case, one can speak of corporate cyber espionage. Economic cyber-espionage potentially presents a security threat because of the political, military and economic harm it can cause. Since information is power, the damage it can inflict is considerable. Yet, espionage and by extension cyber espionage or economic cyber espionage is not per se illegal in international law (with the exception of Art 39 TRIPS agreement) although most national systems criminalise it. Under certain circumstances economic cyber espionage can violate certain international law norms such as those of state-sovereignty and non-intervention. In the following, I will examine the application of the due diligence principle to economic cyber espionage.

The concept of due diligence

Due diligence is a principle of good citizenship which underpins the international legal order. It imposes an obligation on states to respect but also to ensure respect of international law. It places an obligation on states to interfere with private actors and private conduct within their jurisdiction in order to streamline their behaviour in line with the state's international law obligations. The application of this principle to cyberspace is crucial because it overcomes problems concerning attribution and lack of regulation.

The nature and content of the obligation

As this principle has been formulated by the ICJ in the Corfu Channel case, a state has a duty of due diligence not to allow knowingly its territory to be used for acts contrary to the rights of other states.

Due diligence is an obligation of conduct: it demands a certain form of conduct in order for the state to meet its international law obligations.

The obligation of due diligence has two components: the first component refers to capacity and the second to action.

Capacity refers to institutional, resource and jurisdictional capacity. Institutional capacity includes the legal, administrative and institutional mechanisms to allow the state to fulfil its international law obligations. As the Arbitral Tribunal said in the Alabama case, the state cannot hide behind the inadequacies of its domestic system to evade responsibility for lack of diligence

Resource capacity refers to the human, financial and technical resources that will enable a state to act. States need to acquire resources and therefore they need to acquire tools and be acquainted with new technology. Yet, different countries have different resource capacity and international jurisprudence has acknowledged this. In the Tehran hostages case for example, the ICJ found that Iran failed in its due diligence obligation to protect the embassy because it had the resources whereas in the Nicaragua case, the ICJ compared the US with the Nicaraguan resources and exculpated the latter. If lack of resources is an argument put forward by states to justify their failure, due diligence still requires from states to use effectively all available resources or where necessary to prioritise them in order to be able to comply with their obligation.

Finally, jurisdictional capacity is important in the sense that the state needs to exercise control over its territory or over people and activities within its jurisdiction. This extends extraterritorially to territory or spaces under its jurisdiction. The level of control and the ability to control which is conditioned by the available resources are important considerations when issues of responsibility arise as the Nicaragua and the Armed Activities cases reveal but a state needs to employ efforts to acquire such control. This is important in cyberspace, due to its borderless nature and due to the fact that multiple actors operate and multiple activities can take place simultaneously.

The second component of due diligence refers to action in that the state should use the available capabilities when the situation so demands. Moreover, the state should exercise vigilance as to be able to act when the situation so demands. As the ICJ put it in the Pulp Mills case, due diligence entails not only the adoption of appropriate rules and measures but also a certain level of vigilance in their enforcement.

As far as economic cyber espionage is concerned, states should pass new legislation or adapt existing legislation in order to protect trade secrets and IP rights, protect critical infrastructure, ensure cyber hygiene by state and private actors, adopt response and recovery policies. States should also ensure enforcement of the laws through effective investigation and prosecution. States need to provide remedies that may go beyond criminal law remedies. States need to create a framework where information is shared among the multiple stakeholders, private or public. States need to provide training and education. All of the above may require the establishment of new agencies or bodies. States need to acquire, renew and adapt resources, keep abreast of developments, allocate efficiently resources and prioritise available resources. States also needs to exercise control over cyber infrastructure and ensure that they maintain such control by enhancing its monitoring. Finally, states need to respond when incidents to terminate or mitigate them.

Knowledge

Although the obligation of due diligence is assessed by capacity, it is triggered and is particularised by knowledge that a wrongful act has been committed or knowledge of the risk that a wrongful act may be committed.

Knowledge can be actual but this is quite difficult in the cyber environment because of its anonymity, the possibility of spoofing and the clandestine nature of cyber espionage. Circumstantial knowledge may then be used. In the Corfu Channel case the ICJ derived knowledge from certain circumstantial evidence for example the fact that Albania kept a close watch over the Channel. In cyberspace, such evidence for example may refer to the time, place, target, motivation, origin operation

The next question is whether knowledge can be presumed or constructed. In the Corfu Channel case, the Court peregrinated between constructive and presumed knowledge, from an 'ought to know' and 'should have known' standard to a must have known standard. A 'must have known' standard presumes knowledge on the basis of objective facts. Yet, the better view is that the ICJ employed constructive knowledge. The Court rejected the argument that Albania knew of the mining because it exercised territorial control. Instead, according to the ICJ, the lapse of time between the mining and the explosions would have allowed Albania to acquire knowledge had it acted diligently. Judge Azevedo spoke of Albania's failure to place look-out posts that would have allowed her to discover the placement of mines whereas Judge Krylov opined that Albania acted diligently as far as the organisation and functioning of the Albanian cost was concerned and therefore would not bear responsibility. In the same vein, the ICJ constructed knowledge of the genocidal events in the Bosnia Genocide case on the basis of the widespread coverage of the events combined with evidence of personal conversation between President Milosevic and General Mladic.

Thus, the state needs to exercise due diligence to acquire knowledge of events or of risks. In cyberspace it means monitoring infrastructure and activities, good quality intelligence and information as well as mechanisms (technical, forensic, legal, political) and processes for good analysis and evaluation of such information. In contrast, the 'must have known' standard presumes knowledge from facts but states may act in such a way as to avoid the presumption of knowledge, for example states may fail to monitor their infrastructure because monitoring or the exercise of control over infrastructure may presume knowledge

As was said, knowledge particularises the duty of due diligence in that the state needs to act by using all available mechanisms to prevent, terminate or mitigate the particular harm. For example, in the Corfu Channel case, Albania, having acquired knowledge of the mines, she should have warned ships of the existence of mines.

Proof of knowledge is difficult to acquire and even more so in cyberspace. Whereas there may be proof that an act has been committed, proof of who did it may be lacking or, in clandestine operations, what may be lacking is proof of what happened. In short, what is required is proof of the material aspects of an act (economic cyber espionage) but also proof of who did it which in cyberspace requires proof of what

computer/server was involved, its geolocation, who operated it and what are the relations of that person with a state. Standards of evidence may differ depending on whether evidence is presented for political or legal purposes but even l with regard to the latter, international courts often lay down their own evidentiary rules and standards. There are some common themes however that arise from the jurisprudence of the ICJ: (i) control over territory, people or infrastructure provides prima facie evidence but does not prove knowledge without more and does not shift the burden of proof; (ii) widespread reports are not proof of knowledge of a fact. As the ICJ said in the *Nicaragua case* widespread reports of a fact may prove on closer examination to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than the original source; (iii) evidence cannot be presumed even where difficulties in collecting evidence exist. As the ICJ said in the Nicaragua case, it cannot apply a presumption that evidence which is unavailable would, if produced, have supported a particular party's case; still less a presumption of the existence of evidence which has not been produced; (iv) although there is no clear standard of evidence, the ICJ has aligned the standard of evidence to the gravity of the claim. With regard to use of force, clear and convincing evidence is needed which perhaps implies a lower standard for other operations. In the *Bosnian Genocide* Judgment, the Court also appeared to make a distinction between a violation of the prohibition of committing acts of genocide, for which evidence must be 'fully conclusive', and a violation of the obligation to prevent acts of genocide, where the Court required 'proof at a high level of certainty appropriate to the seriousness of the allegation'. From this one may say that a lower standard is required when omissions are involved because it is difficult to establish negative facts but still there is no clear rule as to what evidence is needed to establish what should have been done; (v) the ICJ also accepted a more liberal approach to evidence when evidence is under the opponent's control; (vi) evidence produced through espionage or surveillance even if these activities may violate international law are not inadmissible. In fact, in the Corfu Channel case, the ICJ accepted evidence collected in operations that fro the Court were violations of the non-intervention rule and of sovereignty.

Standard of due diligence

Being an obligation of conduct, due diligence requires from a state to employ its 'best possible efforts' or to take all practicable measures or to take all means reasonable available to prevent or minimise the risk of a wrongful act occuring. The state fails in its duty if it fails to acquire capacity or knowledge that will allow it to fulfil its duty or fails to employ all measures in its power having capacity and knowledge even if the state can prove that the harm would not have been prevented had it taken all reasonable measures. The state also fails if it takes insufficient action.

It transpires from the above that the obligation of due diligence is a variable obligation that depends on capacity (institutional, resource and jurisdictional) as well as on technological developments.

If due diligence constructs differentiated obligations with more advanced states having an enhanced obligation, does it mean that there cannot be any uniform standard against which due diligence can be assessed? In my view, there needs to be a common standard because, otherwise, private or public actors will operate from states with lesser capabilities and in doing so jeopardise international law.

In this regard it should be noted that international law moved away from the diligentia quam in suis principle where diligence was measured against the diligence afforded by the state internally. It is now assessed against an international standard which is commensurate to the international obligation that the state should ensure respect of. Whereas the diligentia quam in suis principle protected states from any external interference, the international standard exposes states to international practice. The state may be afforded some discretion as to how to fulfil its due diligence obligation but it needs to take all 'reasonable' measures to fulfil the obligation. The standard therefore is that of a reasonable state in view of its particular circumstances and in view of the obligation in question.

The situation however is different when specific conventions or regulatory regimes provide for specific actions as it is the case with terrorism where the relevant SC resolutions and anti-terrorism conventions impose obligations on states to adopt specific measures in order to prevent terrorism whereas the CTC engages in capacity building. This is not the case however as far as economic cyber espionage is concerned.

Due diligence and state responsibility

Traditionally, if a state fails in its due diligence obligation, it can be held responsible for such failure. Although international law does not proscribe cyber espionage, when espionage amounts to a violation of the sovereignty of another state or constitutes unlawful intervention, the due diligence obligation is triggered.

Yet, the question remains as to whether the state can also be held responsible for the wrongful act committed by a non-state actor. In tort law, an omission can lead to responsibility for the resultant act if the omission was the cause of such act or, in other cases, if the omission occasioned the act. More specifically, although the wrongful act is committed by a third person, it is the expected consequence of the omission. In the Corfu Channel case for example, the Court found that Albania had a general duty of due diligence which included an obligation to prevent any damage from the moment it learned about the existence of mines. Because Albania failed to act, it was responsible not just for dereliction of diligence but for the explosions and the damage and loss of life that resulted from its lack of diligence. Likewise, command responsibility as formulated in the ICC Statute is responsibility for the crimes of subordinates caused by the superior's failure to prevent their commission.

Can this construction apply to cyber espionage? It is important to note that in both cases –causation or occasioning- there needs to be a specific obligation to prevent the specific harm whereas failure to fulfil the obligation may cause or occasion the harm. In the Corfu Channel case for example the Court found a specific obligation to prevent and in command responsibility there is a specific obligation to prevent. The same can be said with regard to terrorism since the SC resolutions as well as the counter terrorism treaties impose a specific obligation to prevent. Since no such obligation exists as far as cyber espionage is concerned, the above construction cannot apply. If a specific treaty is adopted which requires from states to prevent non-state actors from engaging in economic cyber espionage, the state's failure in this regard may be treated as causing or occasioning the wrongful act.

Due diligence and injury to interests

As was said, the due diligence obligation arises when there is a breach of an obligation owned to another state. If however the particular activity does not constitute a breach of an international obligation - espionage does not in general constitute such a breach- would the failing state be held liable or even responsible if the action caused damage or injured interests?

Firstly, according to Art 39 ASR, the failing state may be liable to pay reparation if its negligent action or omission contributed to the damage.

Secondly, if the act does not constitute a breach of an obligation owned to another state but only affects an interest of the other state or of its citizens, one can claim that the negligent state breached the principle of good faith and, more particularly, that its conduct amounts to abuse of rights. The principle of abuse of rights refers to the mischievous exercise of a right that causes injury to other states but which does not constitute a violation of their rights. The principle of abuse of rights is particularly relevant in areas where state rights are general and discretionary as for example is the right to sovereignty or in areas that are not fully regulated as is the cyberspace or areas of common concern as is perhaps the cyberspace. It requires from states to exercise their rights with due regard to the rights and interests of other states and not to misuse them for the detriment of other states.

Due diligence obligations of non-state actors

There is a due diligence obligation on states to ensure that non-state actors under their jurisdiction are international law compliant Corporations need to exercise appropriate due diligence in order to become aware of, prevent or redress acts that violate a state's international law obligations. This is not however an international law but a national law obligation. If the state has adopted laws to ensure compliance by private person, it has exercised its due diligence and it cannot be held responsible for their acts.

In human rights law, states may be held responsible for the wrongful act committed by third parties. More specifically, states may be held responsible for violating their human rights obligations if the violation that was committed by a third party has transpired because of lack of protection by public authorities (as in Velasquez Rodriguez).

Yet whether this construction constitutes customary human rights law or outside human rights law is debated.

Due diligence obligation to mitigate harm

Does the state which has been affected by economic cyber espionage have a due diligence obligation to mitigate the harm? The affected state has an obligation to take all reasonable measures to stop such activity from the moment it becomes aware thereof. It has also an obligation to mitigate the damage caused. Under the principle of contributory negligence, compensation may be reduced if the injured state or private actor has contributed to the damage by failing to demonstrate diligence. This situation arises from the time the violation and/or damage occurs.

Beginning and end of due diligence obligation

As was said, the due diligence obligation is triggered when the state acquires knowledge of a wrongful act or of the risk that a wrongful act may be committed. Yet knowledge of activities is difficult to acquire particularly of cyber activities. The ICJ in the Genocide case opined that the due diligence obligation with regard to wrongful activities of individuals arises from the moment the state can influence effectively these activities. The obligation of due diligence is continuous; it arises from before the event and carries through after the event but when there is a particular incident due diligence is also particularised. More specifically the state needs to take measure to terminate the wrongful act, mitigate the harm, investigate and punish but also review its capacity.

Economic cyber espionage and international law reform

Any impetus for creating international law on economic cyber espionage is not apparent because of the different interests of stakeholders: states and the private sector. Moreover, cyber espionage or economic cyber espionage may be frowned upon but it is practiced by states which thus prefer to criminalise it under domestic law but not to have any international law proscription. If however states decide to negotiate a treaty, the treaty should define economic cyber espionage, define prohibited activities and

provide for jurisdiction. Such a treaty needs to involve the private sector but international law is not familiar with involving non-state actors in treaties.

My projection is the development of soft law on rules of responsible cyber behaviour which will be general, not focused on cyber espionage, because it is difficult to decipher and recognise different types of cyber activities. Many regional organisations such as the EU or the AU and many national cyber security policies mention rules of cyber behaviour as well as international cooperation.

Questions

What capacity do states need to build in order to be compliant with their due diligence obligation?

What action do states need to take in order to be complaint with their due diligence obligation?

What circumstantial evidence can prove knowledge of economic cyber espionage?

What is the standard of evidence and who has the burden of proof?

What is the 'due' standard in diligence?

Is there an obligation to cooperate with other states to acquire capacity?

Do non-state actors have due diligence obligations?

How can due diligence in this regard be reconciled with human rights or business innovation?

Can a state be responsible for injury to interests?

What should the rules of diligent cyber behaviour be?