

Cybercrime and its Relation to the Principle of Due Diligence

Graham Overcash

As cybercrime, which is “any illegal activity carried out using computers or the internet,” becomes more prevalent in day-to-day life states, individuals, and private businesses are having to adapt to a host of new threats.¹ The nature of cybercrime and the internet allows criminals based anywhere in the world to steal money or damage infrastructure in the United States or elsewhere. Domestic criminal justice systems have shown to be the most effective at preventing and prosecuting cybercriminals, this is especially true when these domestic systems are working together within a larger international framework. The principal international law of due diligence, and treaties such as the Budapest Convention on Cybercrime, encourage states to use domestic systems to prevent international cybercrime.

On October 26, 1946, two British cruisers, accompanied by supporting destroyers, were transiting the Corfu Channel off the coast of Albania in a mine-free zone. Tensions between the British and Albanians were high after Albanian shore batteries fired on two British destroyers in May 1946.² The Albanian batteries missed, and tragedy was narrowly avoided. The flotilla in October was transiting the channel “in order to test the Albanian attitude, that is to say, to see whether the ships would be allowed to pass without interference.”³ The British ships had orders to return fire if fired upon, however, their guns were not loaded.⁴ While off the Albanian coast, the *HMS Saumarez* struck a mine and “was heavily damaged.”⁵ As the *HMS Volage* attempted to tow it to safety, it too struck a mine.⁶ Despite suffering serious damage, the *HMS Volage* was able to tow the *HMS Saumarez* back to port.⁷ In all, eighty-four British seamen were killed that day.⁸

The British began a mine-clearing operation in the wake of this incident. This operation removed over twenty mines from the channel and revealed that the mines were part of a “deliberately laid ... minefield.”⁹ Furthermore, the German-made mines “were laid only a very short time before” the British cruisers hit them.¹⁰ When these facts are taken together, the British government “was certain that no mine field could have been laid in the channel within a few

¹ U.S. Dep’t of Homeland Sec., *Cybercrime Investigations*, <https://www.dhs.gov/hsi/investigate/cybercrime> (last visited Oct. 26, 2024).

² Simon Bronitt, *Australia’s Legal Response to Terrorism: Neither Novel nor Extraordinary?*, 9 AUSTL. J. LEGAL HIST. 49 (2005), available at <https://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/AJLH/2005/3.html> [<https://perma.cc/KC4R-57DH>].

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

hundred yards of the Albanian shore batteries without the connivance, or at least the knowledge, of the Albanian authorities.”¹¹ After a diplomatic back-and-forth between the United Kingdom and the Albanians, the United Kingdom sued Albania in the International Court of Justice (ICJ) to resolve this dispute.

The Court ruled that “it is every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.”¹² The Court noted that “nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania.”¹³ As a well-recognized principle in international law, due diligence is “a standard of reasonableness, of reasonable care, that seeks to take account of the consequences of wrongful conduct and the extent to which such consequences could feasibly have been avoided by the State ... that either commissioned the relevant act or which omitted to prevent its occurrence.”¹⁴ In other words, states must do their best to prevent their territory from being used in an attack, or other wrongful act, on another state.

The principle of due diligence can apply in multiple contexts. The *UN GGE 2015 Norms of Responsible State Behaviour* provides that “[s]tates should not knowingly allow their territory to be used for internationally wrongful acts using (Information and Communications Technology) ICTs.”¹⁵ In the cyberspace context, a “[s]tate must exercise due diligence in not allowing its territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.”¹⁶ Due diligence requires “at a minimum that a state take all measures that are feasible in the circumstances to put an end to cyber-operations conducted from its territory or by persons within its jurisdiction that affect a right of, and produce serious adverse consequences for, other states.”¹⁷

Due diligence measures depend on what is “feasible” in a given circumstance. Relevant factors in determining feasibility are “the capacity of the state concerned, the seriousness of the operations as well as the extent to which the state concerned has knowledge of the operations.”¹⁸ Some states, such as Ireland, consider that “constructive knowledge, often described as a situation where a state ‘ought to have been aware,’ is capable of satisfying the knowledge component of the

¹¹ *Id.*

¹² *Corfu Channel (U.K. v. Alb.)*, Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

¹³ *Id.* at 23.

¹⁴ Tim Stevens and Duncan French, INTERNATIONAL LAW ASSOCIATION, *Study Group on the Conduct of Hostilities and International Humanitarian Law: Draft Report* (2016), https://www.ila-hq.org/en_GB/documents/draft-study-group-report-johannesburg-2016 [<https://perma.cc/B4MJ-QGXP>].

¹⁵ U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 2, U.N. Doc. A/70/174, (July 22, 2015).

¹⁶ *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 30 (Michael N. Schmitt ed., 2d ed. 2017).

¹⁷ *Id.* at Rule 7.

¹⁸ Ireland Dep’t of Foreign Aff., *National Position Paper on International Law and Cyberspace*, at 3 (May 2021).

obligation of due diligence where this can be ascertained to an appropriate level.”¹⁹ In practice, a state cannot monitor and respond to all ICT activity in their country. If the state, however, identifies a risk that actors in their territory intend to conduct cyber operations that could harm another state, then the original state has an obligation to take “reasonable and feasible measures ... to prevent such activities or mitigate their effects.”²⁰ These measures can include domestic law enforcement investigations designed to criminally charge those individuals in a domestic court. This is often the most effective and efficient way to hold cybercriminals accountable and dissuade individuals from engaging in harmful conduct. Domestic criminal justice systems are the first line of defense against cybercrime and provide a way for states to fulfill their due diligence obligations. Moreover, domestic law enforcement agencies and justice systems are better equipped to investigate and prosecute cybercriminals. Domestic organizations do not suffer from issues relating to questions over sovereignty and jurisdiction that international law enforcement organizations and justice systems have. There are, however, times when international cooperation is necessary to prevent cybercrime, mitigate its effects, or hold the perpetrators accountable. The Budapest Convention on Cybercrime urged states to adopt domestic criminal laws to cover various cybercrime such as computer-related fraud/forgery, illegal access, and data interference.²¹

Article 35 of the Budapest Convention on Cybercrime established a 24/7 network to “[facilitate] immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data” among member states.²² This network provides “for expedited international cooperation on cybercrime and electronic evidence between the Parties to the Budapest Convention” that is necessary to prevent and prosecute cybercrimes.²³ Under the convention, states have an obligation to establish a point of contact that provides technical advice, legal information, or assists in collecting evidence to the other member states. The Budapest Convention on Cybercrime is an example of how domestic criminal justice systems must be equipped to investigate and prosecute cybercrimes and countries must be willing to engage in international cooperation in order to respond to cybercrimes.

The principle of due diligence creates obligations for states to take feasible measures to ensure that their territory is not used in the commission of cybercrimes. In order to conform to this principle, states must develop domestic justice systems that are able to investigate and prosecute cybercrimes. To aid these domestic systems, international cooperation is sometimes necessary to investigate these crimes. International treaties like the Budapest Convention highlight the importance of these two ideas in preventing cybercrime from happening. Just as Albania was held

¹⁹ *Id.*

²⁰ *Id.* at 4.

²¹ Convention on Cybercrime of the Council of Europe, Nov. 23, 2001, S. Treaty Doc. No. 108-11, Eur. Treaty Series No. 185, at 18.

²² Eurojust, *24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime*, at 1 (Jan. 23, 2024), <https://www.eurojust.europa.eu/sites/default/files/assets/24-7-points-of-contact-under-article-35-of-the-budapest-convention-on-cybercrime-23-01-2024.pdf> [<https://perma.cc/5V7D-DXDK>].

²³ *Id.*

accountable for failing to prevent harm from its territory, states today bear responsibility for cyber operations originating within their borders.