The due diligence principle is a well-established general principle of international law. The adequacy of its use proved in many special regimes of international law, especially in international environmental law. Cyberspace is another regime where the application of the due diligence principle is desirable. An adequate application of the due diligence principle might mitigate the problem of attribution of cyber operations and help in denying safe havens of non-state actors, who conduct malicious operations in cyberspace. The adequacy of the application of the due diligence principle in cyberspace is further indicated by the results of discussions in international fora and by the emerging trend of support of the application in official declarations of States on the application of international law in cyberspace. The thesis further suggests how the due diligence principle should be applied by introducing three elements that trigger the due diligence obligation and three possible adjustments to them. It also identifies the essence of some controversial aspects of the application of the due diligence principle and introduces cyber-specific considerations for the determination of breaches of the due diligence obligation and evaluation of lawfulness of responses to the breach, which consist of acts of retorsion and countermeasures. Lastly, it explains why the principle of prevention, which forms part of due diligence in international environmental law, is not transferable to the cyber context, and what is the role of private entities in relation to the due diligence principle.