The term cyber warfare refers to means and methods of warfare that rely on information technology and are used in situations of armed conflict. Cyber operations may be either offensive or defensive. IHL only applies to cyber operations that occur during – or that themselves trigger – an armed conflict.

Given the nature of cyber warfare, there is some debate as to whether all cyber attacks trigger the applicability of IHL and – a distinct but related question – whether they constitute “attacks” for the purposes of IHL. Is it necessary, for example, for cyber attacks to result in physical consequences such as the destruction of objects or injury or death of persons? Some argue that acts resulting in mere destruction of data, such as, for instance, interference with information systems, should also be considered as triggering the applicability of IHL and amounting to attacks at least if they have a considerable effect upon the targeted party (an example could be an attack that disabled nationwide banking systems). Cyber attacks that may be regarded as “attacks” within the meaning of IHL must comply with the principles of distinction, proportionality and precautions.

See Conduct of hostilities; Means of warfare; Methods of Warfare; Weapons; Attacks;
Iran, Victim of Cyber warfare

ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts in 2015 (paras 196-221)

BIBLIOGRAPHIC RESOURCES


KELSEY Jeffrey T. G., “Hacking Into International Humanitarian Law: the


Links