Research Handbooks in International Law series

Edited by Nicholas Tsagourias and Russell Buchan

Chapter 12: Self-defence in cyberspace

Carlo Focarelli

Abstract

Is self-defence against a cyber attack permitted? What about a cyber counter-attack against a conventional or cyber attack? Under Article 51 UN Charter self-defence is permitted 'if an armed attack occurs'. Many scholars agree that a cyber attack amounts to an 'armed attack' when it causes harm or damage approximately comparable to a 'kinetic' or conventional attack and in particular when it hits 'critical infrastructures'. Also in cyberspace, when permitted, individual or collective self-de¬fence has to meet the requirements of necessity, proportionality and immediacy. Two further major problems linked with self-defence against cyber attacks discussed in this chapter relate to the permissibility of anticipatory self-defence and self-defence against non-state actors or against the breach by a state of its duty of prevention of cross-border harmful private acts. The chapter concludes with some scepticism about the 'use of force' and analogy-based approaches in the literature suggesting that the law enforcement paradigm and non-forcible responses are preferable to the escalating militarization of cyberspace and noting that even when self-defence is permitted in cyberspace the necessity requirement demands of states to abide by a continuing obligation to implement passive and active electronic defences. In any case the prevailing approach serves, in addition to trying to identify reasonable rules, a twofold purpose, that is, deterring possible attacks and promoting the rules which could possibly govern major cyber attacks at the moment when they occur so as to have at that very moment the international community 'prepared' to share the view that the attack is indeed 'equivalent' to a kinetic attack which justifies a kinetic response.

10. Kesan J.P. & Hayes C.M. Self Defense in Cyberspace: Law and Policy, illinois Public law and legal Theory research Paper series No. 11-16 (2011). 11. Koh H.H. International Law in Cyberspace, Yale law school Faculty scholarship series, Paper 4854 (2012). 12. lewis J.A. A Note on the Laws of War in Cyberspace, Center for strategic and inter-national studies (April 2010). 13. Li S. When Does Internet Denial Trigger the Right of Armed Self-Defense?, 38(1) Yale Journal of international law 179 (2013). 14. Lotriónte C. State Sovereignty and Self-defense in Cyberspace: A Normative Frame-work Second, in cyberspace as in other spaces, states remain sovereign, with rights fully recognized in the U.N. Charter. Even if states recognize the severity and agree on the nature of the cyber threats, they will likely not surrender their fundamental rights. States will still have all the rights of statehood to include the ability to determine whether and to what extent the state will engage with the international community on any security issues. States will maintain the right to use force in self-defense in cyberspace. Just as the U.N. Charter recognizes a state's right of sovereignty, the Charter and customary international law fully recognize a state's right of self-defense against threats. 25U.N. Charter arts. 2, 51. Yet in cyberspace, legitimate self-defense, in practice, is currently defined largely by only one parameter: the boundary of the network. Thus, actions whose effects are confined solely to the defender's network are generally fair game under CFAA, while potentially any effect on the system of the attacker or a third-party risks violating the legal prohibition on accessing another computer "without authorization." Some active defense measures, like beaconing, ought to be considered noncontentious, whereas others, like the kind of "digital booby trap" described by Gregory Falco and Herb Lin, wou