

CS 263 – Alternatives

Alternative Class Activity [contributed by Marion Boulicault]

Students are asked to consider how commonplace metaphors and stereotypes might impact the perception and ethical evaluation of the module's central case study: Facebook security team's 2011 response to ongoing cyberattacks perpetrated by the so-called "Koobface Gang." The Embedded EthiCS TA begins by posing a set of question to the class to try and identify the kinds of background metaphors that pervade ethical debates over hacking back. Examples include questions like "How would you describe what an average hacker looks like? What do you imagine their lifestyle to be like?" and "In the readings for today's class, how was the act of hacking back described? What was it often compared to?" During the discussion, the Embedded EthiCS Fellow writes the answers on the board: hackers are almost always imagined to be male, and usually thought to be misfits or outcasts, sometimes described as successful and powerful and sometimes as living a solitary life in front of screens in a dark basement. The world of 'hacking back' is described often as the "Wild West" and ideas of "vigilantes" evoke images of men with guns. After these metaphors, tropes, and stereotypes are identified, students are split into groups of three to discuss how these metaphors might impact our ethical intuitions about the Koobface case study. They are also asked to come up with alternative descriptions and consider whether we might view cases of hacking back differently if these alternative metaphors were in place. The overall aim of the activity is to help the students understand how ethics is embedded not only in technologies and arguments, but also in the descriptive language we use for describing technologies and making arguments.