World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:05, 2017

Conceptualizing the Cyber Insecurity Risk in the Ethics of Automated Warfare

Authors : Otto Kakhidze, Hoda Alkhzaimi, Adam Ramey, Nasir Memon

Abstract : This paper provides an alternative, cyber security based a conceptual framework for the ethics of automated warfare. The large body of work produced on fully or partially autonomous warfare systems tends to overlook malicious security factors as in the possibility of technical attacks on these systems when it comes to the moral and legal decision-making. The argument provides a risk-oriented justification to why technical malicious risks cannot be dismissed in legal, ethical and policy considerations when warfare models are being implemented and deployed. The assumptions of the paper are supported by providing a broader model that contains the perspective of technological vulnerabilities through the lenses of the Game Theory, Just War Theory as well as standard and non-standard defense ethics. The paper argues that a conventional risk-benefit analysis without considering ethical factors is insufficient for making legal and policy decisions on automated warfare. This approach will provide the substructure for security and defense experts as well as legal scholars, ethicists and decision theorists to work towards common justificatory grounds that will accommodate the technical security concerns that have been overlooked in the current legal and policy models.

Keywords : automated warfare, ethics of automation, inherent hijacking, security vulnerabilities, risk, uncertainty
Conference Title : ICCWS 2017 : International Conference on Cyber Warfare and Security
Conference Location : Barcelona, Spain
Conference Dates : May 26-27, 2017