Similar to the NLP process ([Teufl et. al., 2010](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1007_978-3-642-14706-7_20)) call the process Machine Language Processing (MLP). ([Teufl et. al., 2010](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1007_978-3-642-14706-7_20)) use the e-Participation analysis architecture, extract the various NLP techniques and adopt them for the malware analysis process. ([Kolosnjaji et. al., 2017](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1109_ijcnn.2017.7966340)) transfer the performance improvements achieved in the area of neural networks to model the execution sequences of disassembled malicious binaries. ([Jang et. al., 2017](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1145_3134600.3134635)) present a simple gradient-descent based algorithm for finding adversarial samples, which performs well in comparison to existing algorithms. ([Huang et. al., 2017](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1145_3052973.3053017)) design Gossip, a novel approach to automatically detect malicious domains based on the analysis of discussions in technical mailing lists (particularly on security-related topics) by using natural language processing and machine learning techniques. In order to reduce the manpower of feature engineering prior to the condition of not to extract pre-selected features ([Huang et. al., 2017](https://www.paperdigest.org/paper/?paper_id=arxiv-1705.04448)) develop a coloR-inspired convolutional neuRal networks (CNN)-based AndroiD malware Detection (R2-D2) system. ([Wang et. al., 2018](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1109_tifs.2017.2771228)) propose an effective and automatic malware detection method using the text semantics of network traffic. The approach assessed is a novel dynamic malware analysis method, which may generalize better than static analysis to newer variants ([Kim, 2018](https://www.paperdigest.org/paper/?paper_id=arxiv-1802.05412)). ([Sewak et. al., 2018](https://www.paperdigest.org/paper/?paper_id=arxiv-1809.05889)) investigate and compared one of the Deep Learning Architecture called Deep Neural Network (DNN) with the classical Random Forest (RF) machine learning algorithm for the malware classification. Similar to natural language processing ([Lu, 2019](https://www.paperdigest.org/paper/?paper_id=arxiv-1906.04593)) propose a novel and efficient approach to perform static malware analysis, which can automatically learn the opcode sequence patterns of malware. Other influential work includes ([Kolosnjaji et. al., 2016](https://www.paperdigest.org/paper/?paper_id=doi.org_10.1007_978-3-319-50127-7_11)).