WHAT IS CLAIMED IS:

1. A method comprising:

a) determining, by a data processor, that a malicious computer uses a machine learning model with a boundary function for classification of input data in order to determine outcomes;

b) generating, by the data processor, normal data, wherein the normal data includes typical input data corresponding to the type of machine learning model;

c) providing, by the data processor, the normal data to the malicious computer;

d) obtaining, by the data processor, classification data from the malicious computer, wherein the malicious computer uses the machine learning model to generate the classification data based on the normal data;

e) determining, by the data processor, based on the classification data, characteristics of the machine learning model of the malicious computer;

~~b)~~ f) generating, by the data processor, based on the characteristics of the machine learning model of the malicious computer, transition data to be used as an input to the machine learning model and intended to shift the boundary function;

~~c)~~ g) providing, by the data processor to the malicious computer, the transition data; and

~~d)~~ h) repeating, by the data processor, steps ~~b)~~ f) and ~~c)~~g), thereby causing the boundary function to shift over time.

~~2. The method of claim 1 further comprising:~~

~~generating, by the data processor, normal data;~~

~~providing, by the data processor, the normal data to the malicious computer; and~~

~~determining, by the data processor, characteristics of the machine learning model of the malicious computer.~~

23. The method of claim 12, wherein the characteristics of the machine learning model include separations between clusters of different training data points, an estimate of the boundary function, or a plurality of labels assigned to the normal data.

34. The method of claim 23, wherein the machine learning model is a support vector machine, wherein the boundary function is a hyperplane, and wherein the hyperplane separates a plurality of classifications.

45. The method of claim 34, wherein the plurality of labels are associated with the plurality of classifications.

56. The method of claim 45, wherein the boundary function shifts causing the plurality of classifications to shift.

67. The method of claim 12, wherein generating the normal data further comprises:

retrieving, by the data processor, the normal data from a data source; and

classifying, by the data processor, the normal data.

78. The method of claim 1, wherein the transition data includes data items that share characteristics of data belonging to more than one classification.

89. The method of claim 1, wherein providing the transition data further comprises:

providing, by the data processor, the transition data to a data source, wherein the malicious computer retrieves the transition data from the data source.

910. The method of claim 1, wherein the machine learning model includes linear regression, logistic regression, decision trees, support vector machines, naive Bayes, kNN, K-means, or random forests.

1011. A data processor comprising:

a processor;

a memory device; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

a) determining that a malicious computer uses a machine learning model with a boundary function for classification of input data in order to determine outcomes;

b) generating normal data, wherein the normal data includes typical input data corresponding to the type of machine learning model;

c) providing the normal data to the malicious computer;

d) obtaining classification data from the malicious computer, wherein the malicious computer uses the machine learning model to generate the classification data based on the normal data;

e) determining based on the classification data, characteristics of the machine learning model of the malicious computer;

~~b)~~ f) generating transition data intended to shift the boundary function;

~~c)~~ g) providing, to the malicious computer, the transition data; and

~~d)~~ h) repeating steps ~~b)~~ f) and ~~c)~~g), thereby causing the boundary function to shift over time.

~~12. The data processor of claim 11, wherein the method further comprises:~~

~~generating normal data;~~

~~providing the normal data to the malicious computer; and~~

~~determining characteristics of the machine learning model of the malicious computer.~~

11~~13~~. The data processor of claim 10~~12~~, wherein the characteristics of the machine learning model include separations between clusters of different training data points, an estimate of the boundary function, or a plurality of labels assigned to the normal data.

12~~14~~. The data processor of claim 11~~13~~, wherein the machine learning model is a support vector machine, wherein the boundary function is a hyperplane, and wherein the hyperplane separates a plurality of classifications.

13~~15~~. The data processor of claim 12~~14~~, wherein the plurality of labels are associated with the plurality of classifications.

14~~16~~. The data processor of claim 13~~15~~, wherein the boundary function shifts causing the plurality of classifications to shift.

15~~17~~. The data processor of claim ~~12~~ 10, wherein generating the normal data further comprises:

retrieving the normal data from a data source; and

classifying the normal data.

16~~18~~. The data processor of claim 10~~11~~, wherein the transition data includes data items that share characteristics of data belonging to more than one classification.

1719. The data processor of claim 1011, wherein providing the transition data further comprises:

providing the transition data to a data source, wherein the malicious computer retrieves the transition data from the data source.

1820. The data processor of claim 1011, wherein the machine learning model includes linear regression, logistic regression, decision trees, support vector machines, naive Bayes, kNN, K-means, or random forests.