

CLAIMS:

1. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Critical Infrastructure Protection & Retribution (CIPR) through Cloud & Tiered Information Security (CTIS), further comprising:
 - a) Trusted Platform, which comprises network of agents that report hacker activity;
 - b) Managed Network & Security Services Provider (MNSP), which provides Managed Encrypted Security, Connectivity & Compliance Solutions & Services;wherein virtual private network (VPN) connects the MNSP and the Trusted Platform, wherein VPN provides a communication channel to and from the Trusted Platform, wherein the MNSP is adapted to analyze all traffic in the enterprise network, wherein the traffic is routed to the MNSP, wherein the MNSP comprises:
 - a) Logically Inferred Zero-database A-priori Realtime Defense (LIZARD), which derive purpose and functionality from foreign code, and hence block it upon presence of malicious intent or absence of legitimate cause, and analyzes threats in and of themselves without referencing prior historical data;
 - b) Artificial Security Threat (AST), which provides a hypothetical security scenario to test an efficacy of security rulesets;
 - c) Creativity Module, which performs process of intelligently creating new hybrid forms out of prior forms;
 - d) Conspiracy Detection, which discerns information collaboration and extracts patterns of security related behavior and provides a routine background check for multiple conspiratorial security events, and attempts to determine patterns and correlations between seemingly unrelated security events;
 - e) Security Behavior, which stores and indexes events and their security responses and traits, wherein a response comprises block/approval decisions;

- f) Iterative Intelligence Growth / Intelligence Evolution (I²GE), which leverages big data and malware signature recognition, and emulates future potential variations of Malware by leveraging the AST with the Creativity Module; and
- g) Critical Thinking, Memory, Perception (CTMP), which criticizes the block/approval decisions and acts as a supplemental layer of security, and leverages cross-references intelligence from I²GE, LIZARD, and Trusted Platform, wherein CTMP estimates its own capacity of forming an objective decision on a matter, and will refrain from asserting a decision made with internal low confidence.

2. The system of claim 1, wherein a LIZARD Lite Client, which is adapted to operate in a device of the enterprise network, securely communicates with the LIZARD in the MNISP.

3. The system of claim 1, further comprises Demilitarized Zone (DMZ), which comprises a subnetwork which contains an HTTP server which has a higher security liability than a normal computer so that the rest of the enterprise network is not exposed to such a security liability.

4. The system of claim 1, wherein the I²GE comprises Iterative Evolution, in which parallel evolutionary pathways are matured and selected, iterative generations adapt to the same Artificial Security Threats (AST), and the pathway with the best personality traits ends up resisting the security threats the most.

5. The system of claim 1, wherein the LIZARD comprises:

- a) Syntax Module, which provides a framework for reading & writing computer code;
- b) Purpose Module, which uses the Syntax Module to derive a purpose from code, and outputs the purpose in its complex purpose format;
- c) Virtual Obfuscation, in which the enterprise network and database is cloned in a virtual environment, and sensitive data is replaced with mock (fake) data, wherein depending on the behavior of a target, the environment can be dynamically altered in real time to include more fake elements or more real elements of the system at large;

- d) Signal Mimicry, which provides a form of Retribution when the analytical conclusion of Virtual Obfuscation has been reached;
 - e) Internal Consistency Check, which checks that all the internal functions of a foreign code make sense;
 - f) Foreign Code Rewrite, which uses the Syntax and Purpose modules to reduce foreign code to a Complex Purpose Format;
 - g) Covert Code Detection, which detects code covertly embedded in data & transmission packets;
 - h) Need Map Matching, which is a mapped hierarchy of need & purpose and is referenced to decide if foreign code fits in the overall objective of the system;
- wherein for writing the Syntax Module receives a complex formatted purpose from the Purpose Module, then writes code in arbitrary code syntax, then a helper function translates that arbitrary code to real executable code; wherein for reading the Syntax Module provides syntactical interpretation of code for the Purpose Module to derive a purpose for the functionality of such code;
- wherein the Signal Mimicry uses the Syntax Module to understand a malware's communicative syntax with its hackers, then hijacks such communication to give malware the false impression that it successfully sent sensitive data back to the hackers, wherein the hackers are also sent the malware's error code by LIZARD, making it look like it came from the malware;
- wherein the Foreign Code Rewrite builds the codeset using the derived Purpose whereby ensuring that only the desired and understood purpose of the foreign code is executed within the enterprise, and any unintended function executions do not gain access to the system.

6. The system of claim 5, wherein for the Foreign Code Rewrite to syntactically reproduce foreign code to mitigate potentially undetected malicious exploits, Combination Method compares and matches Declared Purpose with Derived Purpose, wherein the Purpose Module is used to manipulate Complex Purpose Format, wherein with the Derived Purpose, the Need Map Matching keeps a hierarchical structure to maintain jurisdiction of all enterprises needs whereby the purpose of a block of code can be defined and justified, depending on vacancies in

the jurisdictionally orientated Need Map, wherein Input Purpose is the intake for Recursive Debugging process.

7. The system of claim 6, wherein the Recursive Debugging loops through code segments to test for bugs and applies bug fixes, wherein if a bug persists, the entire code segment is replaced with the original foreign code segment, wherein the original code segment is subsequently tagged for facilitating Virtual Obfuscation and Behavioral Analysis, wherein with Foreign Code, the original state of the code is interpreted by the Purpose Module and the Syntax Module for a code rewrite, wherein the Foreign Code is directly referenced by the debugger in case an original foreign code segment needs to be installed because there was a permanent bug in the rewritten version, wherein at Rewritten Code, Segments are tested by Virtual Runtime Environment to check for Coding Bugs, wherein the Virtual Runtime Environment executes Code Segments, and checks for runtime errors, wherein with Coding Bug, errors produced in the Virtual Runtime Environment are defined in scope and type, wherein with Purpose Alignment, a potential solution for the Coding Bug is drafted by re-deriving code from the stated purpose, wherein the scope of the Coding Bug is rewritten in an alternate format to avoid such a bug, wherein the potential solution is outputted, and wherein if no solutions remain, the code rewrite for that Code Segment is forfeited and the original Code Segment directly from the Foreign Code is used in the final code set.

8. The system of claim 6, wherein for operation of the Need Map Matching, LIZARD Cloud and LIZARD Lite reference a Hierarchical Map of enterprise jurisdiction branches, wherein whether the Input Purpose is claimed or derived via the Purpose Module, the Need Map Matching validates the justification for the code/function to perform within the Enterprise System, wherein a master copy of the Hierarchical Map is stored on LIZARD Cloud in the MNSP, wherein Need Index within the Need Map Matching is calculated by referencing the master copy, wherein then the pre-optimized Need Index is distributed among all accessible endpoint clients, wherein the Need Map Matching receives a Need Request for the most appropriate

need of the system at large, wherein the corresponding output is a Complex Purpose Format that represents the appropriate need.

9. The system of claim 1, wherein an entire LAN infrastructure for the enterprise is reconstructed virtually within the MNSP, wherein the hacker is then exposed to elements of both the real LAN infrastructure and the virtual clone version as the system performs behavioral analysis, wherein if the results of such analysis indicates risk, then the hacker's exposure to the virtual clone infrastructure is increased to mitigate the risk of real data and/or devices becoming compromised.

10. The system of claim 1, wherein Malware Root Signature is provided to the AST so that iterations/variations of the Malware Root Signature is formed, wherein Polymorphic Variations of malware are provided as output from I²GE and transferred to Malware Detection.

11. The system of claim 10, wherein the Malware Detection is deployed on all three levels of a computer's composition, which includes User Space, Kernel Space and Firmware/Hardware Space, wherein all the Spaces are monitored by Lizard Lite agents.

12. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Machine Clandestine Intelligence (MACINT) & Retribution through Covert Operations in Cyberspace, further comprising:

a) Intelligent Information and Configuration Management (I²CM), which provides intelligent information management, viewing and control; and

b) Management Console (MC), which provides input/output channel to users:

wherein the I²CM comprises:

i) Aggregation, which uses generic level criteria to filter out unimportant and redundant information, and merges and tags streams of information from multiple platforms;

- ii) Configuration and Deployment Service, which comprises an interface for deploying new enterprise network devices with predetermined security configuration and connectivity setup and for managing deployment of new user accounts;
- iii) Separation by Jurisdiction, in which tagged pool of information are separated exclusively according to a relevant jurisdiction of a Management Console User;
- iv) Separation by Threat, which organizes the information according to individual threats; and
- v) Automated Controls, which accesses MNSP Cloud, Trusted Platform, or additional Third Party Services.

13. The system of claim 12, wherein in the MNSP Cloud, Behavioral Analysis observes a malware's state of being and actions performed whilst it is in Mock Data Environment; wherein when the Malware attempts to send Fake Data to Hacker, the outgoing signal is rerouted so that it is received by Fake Hacker; wherein Hacker Interface receives the code structure of the Malware and reverse engineers the Malware's internal structure to output Hacker Interface; wherein Fake Hacker and Fake Malware are emulated within a Virtualized Environment; wherein the virtualized Fake Hacker sends a response signal to the real Malware to observe the malware's next behavior pattern, wherein the hacker is given a fake response code that is not correlated with the behavior/state of the real malware.

14. The system of claim 12, wherein Exploit Scan identifies capabilities and characteristics of criminal assets and the resulting scan results are managed by Exploit, which is a program sent by the Trusted Platform via the Retribution Exploits Database that infiltrates target Criminal System, wherein the Retribution Exploits Database contains a means of exploiting criminal activities that are provided by Hardware Vendors in the forms of established backdoors and known vulnerabilities, wherein Unified Forensic Evidence Database contains compiled forensic evidence from multiple sources that spans multiple enterprises.

15. The system of claim 12, wherein when a sleeper agent from a criminal system captures a file of an enterprise network, a firewall generates log, which is forwarded to Log Aggregation, wherein Log Aggregation separates the data categorically for a Long-Term/Deep Scan and a Real-Time/Surface Scan.

16. The system of claim 15, wherein the Deep Scan contributes to and engages with Big Data whilst leveraging Conspiracy Detection sub-algorithm and Foreign Entities Management sub-algorithm; wherein standard logs from security checkpoints are aggregated and selected with low restriction filters at Log Aggregation; wherein Event Index + Tracking stores event details; wherein Anomaly Detection uses Event Index and Security Behavior in accordance with the intermediate data provided by the Deep Scan module to determine any potential risk events; wherein Foreign Entities Management and Conspiracy Detection are involved in analysis of events.

17. The system of claim 15, wherein the Trusted Platform looks up an Arbitrary Computer to check if it or its server relatives/neighbors (other servers it connects to) are previously established double or triple agents for the Trusted Platform; wherein the agent lookup check is performed at Trusted Double Agent Index + Tracking Cloud and Trusted Triple Agent Index + Tracking Cloud; wherein a double agent, which is trusted by the arbitrary computer, pushes an Exploit through its trusted channel, wherein the Exploit attempts to find the Sensitive File, quarantines it, sends its exact state back to the Trusted Platform, and then attempts to secure erase it from the Criminal Computer.

18. The system of claim 17, wherein ISP API request is made via the Trusted Platform and at Network Oversight network logs for the Arbitrary System and a potential file transfer to Criminal Computer are found, wherein metadata is used to decide with significant confidence which computer the file was sent to, wherein the Network Oversight discovers the network details of Criminal Computer and reroutes such information to the Trusted Platform, wherein the Trusted Platform is used to engage security APIs provided by Software and Hardware vendors to exploit any established backdoors that can aide the judicial investigation.

19. The system of claim 12, wherein the Trusted Platform pushes a software or firmware Update to the Criminal Computer to establish a new backdoor, wherein a Placebo Update is pushed to nearby similar machines to maintain stealth, wherein Target Identity Details are sent to the Trusted Platform, wherein the Trusted Platform communicates with a Software/Firmware Maintainer to push Placebo Updates and Backdoor Updates to the relevant computers, wherein the Backdoor Update introduces a new backdoor into the Criminal Computer's system by the using the pre-established software update system installed on the Computer, wherein the Placebo Update omits the backdoor, wherein the Maintainer transfers the Backdoor to the target, as well as to computers which have an above average amount of exposure to the target, wherein upon implementation of the Exploit via the Backdoor Update the Sensitive File is quarantined and copied so that its metadata usage history can be later analyzed, wherein any supplemental forensic data is gathered and sent to the exploit's point of contact at the Trusted Platform.

20. The system of claim 12, wherein a long-term priority flag is pushed onto the Trusted Platform to monitor the Criminal System for any and all changes/updates, wherein the Enterprise System submits a Target to Warrant Module, which scans all Affiliate Systems Input for any associations of the defined Target, wherein if there are any matches, the information is passed onto the Enterprise System, which defined the warrant and seeks to infiltrate the Target, wherein the Input is transferred to Desired Analytical Module, which synchronizes mutually beneficial security information.

21. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Logically Inferred Zero-database A-priori Realtime Defense (LIZARD), further comprising:

- a) Static Core(SC), which comprises predominantly fixed program modules;
 - b) Iteration Module, which modifies, creates and destroys modules on Dynamic Shell, wherein the Iteration Module uses AST for a reference of security performance and uses Iteration Core to process an automatic code writing methodology;
 - c) Differential Modifier Algorithm, which modifies a Base Iteration according to flaws the AST found, wherein after the differential logic is applied, a new iteration is proposed, upon which the Iteration Core is recursively called and undergoes the same process of being tested by AST;
 - d) Logic Deduction Algorithm, which receives known security responses of a Dynamic Shell Iteration from the AST, wherein LDA deduces what codeset makeup will achieve a known Correct Response to a security scenario;
 - e) Dynamic Shell (DS), which contains predominantly dynamic program modules that have been automatically programmed by the Iteration Module (IM);
 - f) Code Quarantine, which isolates foreign code into a restricted virtual environment;
 - g) Covert Code Detection, which detects code covertly embedded in data and transmission packets; and
 - h) Foreign Code Rewrite, which after deriving foreign code purpose, rewrites either parts or a whole code itself and allows only a rewrite to be executed;
- wherein all enterprise devices routed through LIZARD, wherein all software and firmware that runs enterprise devices are hardcoded to perform any sort of download/upload via LIZARD as a permanent proxy, wherein LIZARD interacts with three types of data comprising data in motion, data in use, and data at rest, wherein LIZARD interacts with data mediums comprising Files, Email, Web, Mobile, Cloud and Removable Media.

22. The system of claim 21, further comprising:

- a) AST Overflow Relay, wherein data is relayed to the AST for future iteration improvement when the system can only perform a low confidence decision;
- b) Internal Consistency Check, which checks if all the internal functions of a block of foreign code make sense;

- c) Mirror test, which checks to make sure the input/output dynamic of the rewrite is the same as the original, whereby any hidden exploits in the original code are made redundant and are never executed;
- d) Need Map Matching, which comprises a mapped hierarchy of need and purpose that are referenced to decide if foreign code fits in the overall objective of the system;
- e) Real Data Synchronizer, which selects data to be given to mixed environments and in what priority whereby sensitive information is inaccessible to suspected malware;
- f) Data manager, which is the middleman interface between entity and data coming from outside of the virtual environment;
- g) Virtual Obfuscation, which confuses and restricts code by gradually and partially submerging them into a virtualized fake environment;
- h) Covert Transportation Module, which transfers malware silently and discretely to a Mock Data Environment; and
- i) Data Recall Tracking, which keeps track of all information uploaded from and downloaded to the Suspicious Entity.

23. The system of claim 22, further comprising Purpose Comparison Module, in which four different types of Purpose are compared to ensure that the entity's existence and behavior are merited and understood by LIZARD in being productive towards the system's overall objectives.

24. The system of claim 23, wherein the Iteration Module uses the SC to syntactically modify the code base of DS according to the defined purpose in from the Data Return Relay (DRR), wherein the modified version of LIZARD is stress tested in parallel with multiple and varying security scenarios by the AST.

25. The system of claim 24, wherein inside the SC, Logic Derivation derives logically necessary functions from initially simpler functions whereby an entire tree of function dependencies are built from a stated complex purpose;

wherein Code Translation converts arbitrary generic code which is understood directly by Syntax Module functions to any chosen known computer language and the inverse of translating known computer languages to arbitrary code is also performed;

wherein Logic Reduction reduces logic written in code to simpler forms to produce a map of interconnected functions;

wherein Complex Purpose Format is a storage format for storing interconnected sub-purposes that represent an overall purpose;

wherein Purpose Associations is a hardcoded reference for what functions and types of behavior refer to what kind of purpose;

wherein Iterative Expansion adds detail and complexity to evolve a simple goal into a complex purpose by referring to Purpose Associations;

wherein Iterative Interpretation loops through all interconnected functions and produces an interpreted purpose by referring to Purpose Associations;

wherein Outer Core is formed by the Syntax and Purpose modules which work together to derive a logical purpose to unknown foreign code, and to produce executable code from a stated function code goal;

wherein Foreign Code is code that is unknown to LIZARD and the functionality and intended purpose is unknown and the Foreign Code is the input to the inner core and Derived Purpose is the output, wherein the Derived Purpose is the intention of the given Code as estimated by the Purpose Module, wherein the Derived Purpose is returned in the Complex Purpose Format.

26. The system of claim 25, wherein the IM uses AST for a reference of security performance and uses the Iteration Core to process the automatic code writing methodology, wherein at the DRR data on malicious attacks and bad actors is relayed to the AST when LIZARD had to resort to making a decision with low confidence; wherein inside the Iteration Core, Differential Modifier Algorithm (DMA) receives Syntax/Purpose Programming Abilities and System Objective Guidance from the Inner Core, and uses such a codeset to modify the Base Iteration according to the flaws the AST 17 found; wherein Security Result Flaws are presented

visually as to indicate the security threats that passed through the Base Iteration whilst running the Virtual Execution Environment.

27. The system of claim 26, wherein inside the DMA, Current State represents Dynamic Shell codeset with symbolically correlated shapes, sizes and positions, wherein different configurations of these shapes indicate different configurations of security intelligence and reactions, wherein the AST provides any potential responses of the Current State that happened to be incorrect and what the correct response is; wherein Attack Vector acts as a symbolic demonstration for a cybersecurity threat, wherein Direction, size, and color all correlate to hypothetical security properties like attack vector, size of malware, and type of malware, wherein the Attack Vector symbolically bounces off of the codeset to represent the security response of the codeset;

wherein Correct State represents the final result of the DMA's process for yielding the desired security response from a block of code of the Dynamic Shell, wherein differences between the Current State and Correct State result in different Attack Vector responses;

wherein the AST provides Known Security Flaws along with Correct Security Response, wherein Logic Deduction Algorithm uses prior Iterations of the DS to produce a superior and better equipped Iteration of the Dynamic Shell known as Correct Security Response Program.

28. The system of claim 24, wherein inside Virtual Obfuscation, questionable Code is covertly allocated to an environment in which half of the data is intelligently mixed with mock data, wherein any subjects operating within Real System can be easily and covertly transferred to a Partially or Fully Mock Data Environment due to Virtual Isolation; wherein Mock Data Generator uses the Real Data Synchronizer as a template for creating counterfeit & useless data; wherein perceived risk of confidence in perception of the incoming Foreign Code will influence the level of Obfuscation that LIZARD chooses; wherein High confidence in the code being malicious will invoke allocation to an environment that contains large amounts of Mock Data; wherein Low confidence in the code being malicious can invoke either allocation to a Real System or the 100% Mock Data Environment.

29. The system of claim 28, wherein Data Recall Tracking keeps track of all information uploaded from and downloaded to the Suspicious Entity; wherein in the case that Mock Data had been sent to a legitimate enterprise entity, a callback is performed which calls back all of the Mock Data, and the Real Data is sent as a replacement; wherein a callback trigger is implemented so that a legitimate enterprise entity will hold back on acting on certain information until there is a confirmation that the data is not fake.

30. The system of claim 29, wherein Behavioral Analysis tracks the download and upload behavior of the Suspicious Entity to determine potential Corrective Action, wherein the Real System contains the original Real Data that exists entirely outside of the virtualized environment, wherein Real Data that Replaces Mock Data is where Real data is provided unfiltered to the Data Recall Tracking whereby a Real Data Patch can be made to replace the mock data with real data on the Formerly Suspicious Entity; wherein the Data Manager, which is submerged in the Virtually Isolated Environment, receives a Real Data Patch from the Data Recall Tracking; wherein when Harmless Code has been cleared by Behavioral Analysis to being malicious, Corrective Action is performed to replace the Mock Data in the Formerly Suspicious Entity with the Real Data that it represents; wherein Secret Token is a security string that is generated and assigned by LIZARD allows the Entity that is indeed harmless to not proceed with its job; wherein if the Token is Missing, this indicates the likely scenario that this legitimate entity has been accidentally placed in a partially Mock Data Environment because of the risk assessment of it being malware, thereafter Delayed Session with the Delay Interface is activated; wherein if the Token is found , this indicates that the server environment is real and hence any delayed sessions are Deactivated.

31. The system of claim 29, wherein inside the Behavioral Analysis, Purpose Map is a hierarchy of System Objectives which grants purpose to the entire Enterprise System, wherein the Declared, Activity and Codebase Purposes are compared to the innate system need for whatever the Suspicious Entity is allegedly doing; wherein with Activity Monitoring the

suspicious entity's Storage, CPU Processing, and Network Activity are monitored, wherein the Syntax Module interprets such Activity in terms of desired function, wherein such functions are then translated to an intended purpose in behavior by the Purpose Module, wherein Codebase is the source code/programming structure of the Suspicious Entity and is forwarded to the Syntax Module, wherein the Syntax Module understands coding syntax and reduces programming code and code activity to an intermediate Map of Interconnected Functions, wherein the Purpose Module produces the perceived intentions of the Suspicious Entity, the outputs Codebase Purpose and Activity Purpose, wherein the Codebase Purpose contains the known purpose, function, jurisdiction and authority of Entity as derived by LIZARD's syntactical programming capabilities, wherein the Activity Purpose contains the known purpose, function, jurisdiction and authority of Entity as understood by LIZARD's understanding of its storage, processing and network Activity, wherein the Declared Purpose is the assumed purpose, function, jurisdiction, and authority of Entity as declared by the Entity itself, wherein the Needed Purpose contains the expected purpose, function, jurisdiction and authority the Enterprise System requires, wherein all the purposes are compared in the Comparison Module, wherein any inconsistencies between the purposes will invoke a Divergence in Purpose scenario which leads to Corrective Action.

32. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Critical Thinking Memory & Perception (CTMP), further comprising:

- a) Critical Rule Scope Extender (CRSE), which takes known scope of perceptions and upgrade them to include critical thinking scopes of perceptions;
- b) Correct rules, which indicates correct rules that have been derived by using the critical thinking scope of perception;

- c) Rule Execution (RE), which executes rules that have been confirmed as present and fulfilled as per the memory's scan of a Chaotic Field to produce desired and relevant critical thinking decisions;
- d) Critical Decision Output, which produces final logic for determining the overall output of CTMP by comparing conclusions reached by both Perception Observer Emulator (POE) and the RE;

wherein the POE produces an emulation of an observer and tests/compares all potential points of perception with such variations of observer emulations;

wherein the RE comprises a checkerboard plane which is used to track transformations of rulesets, wherein objects on the checkerboard plane represents a complexity of any given security situation, whilst a movement of such objects across a 'security checkerboard' indicates an evolution of the security situation which is managed by responses of security rulesets.

33. The system of claim 32, further comprising:

- a) Subjective opinion decisions, which decision provided by Selected Pattern Matching Algorithm (SPMA);
- b) Input system Metadata, which comprises raw metadata from the SPMA, which describes the mechanical process of the algorithm and how it reached such decisions;
- c) Reason Processing, which logically understands the assertions by comparing attributes of properties;
- d) Rule Processing, which uses the resultant rules that have been derived are used as a reference point to determine the scope of the problem at hand;
- e) Memory Web, which scans market variables logs for fulfillable rules;
- f) Raw Perception Production, which receives metadata logs from the SPMA, wherein the logs are parsed and a perception is formed that represents the perception of such algorithm, wherein the perception is stored in a Perception Complex Format (PCF), and is emulated by the POE; wherein Applied Angles of Perception indicates angles of perception that have already been applied and utilized by the SPMA;

- g) Automated Perception Discovery Mechanism (APDM), which leverages Creativity Module, which produces hybridized perceptions that are formed according to the input provided by Applied Angles of Perception whereby the perception's scope can be increased;
- h) Self-Critical Knowledge Density (SCKD), which estimates the scope and type of potential unknown knowledge that is beyond the reach of the reportable logs whereby the subsequent critical thinking features of CTMP can leverage the potential scope of all involved knowledge; wherein Critical Thinking indicates the outer shell jurisdiction of rule based thinking;
- i) Implication Derivation (ID), which derives angles of perception data that can be implicated from the current Applied Angles of Perception;

wherein the SPMA is juxtaposed against the Critical Thinking performed by CTMP via perceptions and rules.

34. The system of claim 33, further comprising

- a) Resource Management & Allocation (RMA), in which adjustable policy dictates the amount of perceptions that are leveraged to perform an observer emulation, wherein the priority of perceptions chosen are selected according to weight in descending order, wherein the policy then dictates the manner of selecting a cut off, whether than be a percentage, fixed number, or a more complex algorithm of selection;
- b) Storage Search (SS), which uses the CVF derived from the data enhanced logs as criteria in a database lookup of the Perception Storage (PS), wherein in PS, perceptions, in addition to their relevant weight, are stored with the comparable variable format (CVF) as their index;
- c) Metric Processing, which reverse engineers the variables allocation from the SPMA;
- d) Perception Deduction (PD), which uses the allocation response and its corresponding system metadata to replicate the original perception of the allocation response;
- e) Metadata Categorization Module (MCM), in which the debugging and algorithm traces are separated into distinct categories using syntax based information categorization, wherein the categories are used to organize and produce distinct allocation responses with a correlation to risks and opportunities;
- f) Metric Combination, which separates angles of perception into categories of metrics;

- g) Metric Conversion, which reverses individual metrics back into whole angles of perception;
- h) Metric Expansion (ME), which stores the metrics of multiple and varying angles of perception categorically in individual databases;
- i) Comparable Variable Format Generator (CVFG), which converts a stream of information into Comparable Variable Format (CVF).

35. The system of claim 34, further comprising:

- a) Perception Matching 503, in which CVF is formed from the perception received from Rule Syntax Derivation (RSD); wherein the newly formed CVF is used to lookup relevant Perceptions in the PS with similar indexes, wherein the potential matches are returned to Rule Syntax Generation (RSG);
- b) Memory Recognition (MR), in which a Chaotic Field 613 is formed from input data;
- c) Memory Concept Indexing, in which the whole concepts are individually optimized into indexes, wherein the indexes are used by the letter scanners to interact with the Chaotic Field;
- d) Rule Fulfillment Parser (RFP), which receives the individual parts of the rule with a tag of recognition, wherein each part is marked as either having been found, or not found in the Chaotic Field by Memory Recognition; wherein the RFP logically deduces which whole rules, the combination of all of their parts, have been sufficiently recognized in the Chaotic Field to merit the RE;
- e) Rule Syntax Format Separation (RSFS), in which Correct Rules are separated and organized by type whereby all the actions, properties, conditions, and objects are stacked separately;
- f) Rule Syntax Derivation, in which logical 'black and white' rules are converted to metric based perceptions, whereby the complex arrangement of multiple rules are converted into a single uniform perception that is expressed via multiple metrics of varying gradients;
- g) Rule Syntax Generation (RSG), which receives previously confirmed perceptions which are stored in Perception Format and engages with the perception's internal metric makeup,

wherein such gradient based measures of metrics are converted to binary and logical rulesets that emulates the input/output information flow of the original perception;

- h) Rule Syntax Format Separation (RSFS), in which Correct rules represent the accurate manifestation of rulesets that conform to the reality of the object being observed, whereby Correct rules are separated and organized by type and hence all the actions, properties, conditions, and objects are stacked separately enabling the system to discern what parts have been found in the Chaotic Field, and what parts have not;
- i) Innate Logical Deduction, which uses logical principles, hence avoiding fallacies, to deduce what kind of rule will accurately represent the many gradients of metrics within the perception;
- j) Metric Context Analysis, which analyzes the interconnected relationships within the perceptions of metrics, wherein certain metrics can depend on others with varying degrees of magnitude, wherein this contextualization is used to supplement the mirrored interconnected relationship that rules have within the 'digital' ruleset format;
- k) Rule Syntax Format Conversion (RSFC), which assorts and separate rules to conform to the syntax of the Rule Syntax Format (RSF);

wherein Intuitive Decision engages in critical thinking via leveraging perceptions, wherein Thinking Decision engages in critical thinking via leveraging rules, wherein Perceptions is data received from Intuitive Decision according to a format syntax defined in Internal Format, wherein Fulfilled Rules is data received from Thinking Decision, which is a collection of fulfillable rulesets from the RE, wherein the data is passed on in accordance with the format syntax defined in Internal Format;

wherein Actions indicates an action that may have already been performed, will be performed, is being considered for activation, wherein Properties indicates some property-like attribute which describes something else, be it an Action, Condition or Object, wherein Conditions indicates a logical operation or operator, wherein Objects indicates a target which can have attributes applied to it;

wherein Separated Rule Format is used as output from the Rule Syntax Format Separation (RSFS), which is considered the pre-Memory Recognition phase, and as output from Memory Recognition (MR), which is considered the post-Memory Recognition phase.

36. The system of claim 35, further comprising:

- a) Chaotic Field Parsing (CFP), which combines the format of the logs into a single scannable Chaotic Field 613;
- b) Extra Rules, which are produced from Memory Recognition (MR) to supplement the Correct Rules;

wherein inside Perception Matching (PM), Metric Statistics provides statistical information from Perception Storage, Error Management parses syntax and/or logical errors stemming from any of the individual metrics, Separate Metrics isolates each individual metric since they used to be combined in a single unit which was the Input Perception, Node Comparison Algorithm (NCA) receives the node makeup of two or more CVFs, wherein Each node of a CVF represents the degree of magnitude of a property, wherein a similarity comparison is performed on an individual node basis, and the aggregate variance is calculated, wherein a smaller variance number represents a closer match.

37. The system of claim 36, further comprising:

- a) Raw Perceptions - Intuitive Thinking (Analog), which processes the perceptions according to an 'analog' format, wherein Analog Format perceptions pertains to the decision are stored in gradients on a smooth curve without steps;
- b) Raw Rules - Logical Thinking (Digital), which processes rules according to a digital format, wherein Digital Format raw rules pertains to the decision are stored in steps with little to no 'grey area';

wherein Unfulfilled Rules are rulesets that have not been sufficiently recognized in the Chaotic Field according to their logical dependencies, and Fulfilled Rules are rulesets that have been recognized as sufficiently available in the Chaotic Field 613 according to their logical dependencies;

wherein Queue Management (QM) leverages the Syntactical Relationship Reconstruction (SRR) to analyze each individual part in the most logical order and has access to the Memory Recognition (MR) results whereby the binary yes/no flow questions can be answered and appropriate action can be taken, wherein QM checks every rule segment in stages, if a single segment is missing from the Chaotic Field and not in proper relation with the other segments, the ruleset is flagged as unfulfilled.

38. The system of claim 37, wherein Sequential Memory Organization is an optimized information storage for 'chains' of sequenced information, wherein in Points of Memory Access, the width of each of the Nodes (blocks) represent the direct accessibility of the observer to the memorized object (node), wherein with Scope of Accessibility each letter represents its point of direct memory access to the observer, wherein a wider scope of accessibility indicates that there are more points of accessibility per sequence node, wherein the more a sequence would be referenced only 'in order' and not from any randomly selected node, the more narrow the scope of accessibility (relative to sequence size, wherein with Nested Sub-Sequence Layers, a sequence that exhibits strong non-uniformity is made up of a series of smaller sub-sequences that interconnect.

39. The system of claim 37, wherein Non-Sequential Memory Organization deals with the information storage of non-sequentially related items, wherein reversibility indicates a non-sequential arrangement and a uniform scope, wherein non-sequential relation is indicated by the relatively wide point of access per node, wherein the same uniformity exists when the order of the nodes is shuffled, wherein in Nucleus Topic and Associations, the same series of nodes are repeated but with a different nucleus (the center object), wherein the nucleus represents the primary topic, to which the remaining nodes act as memory neighbours to which they can be accessed easier as opposed to if there were no nucleus topic defined.

40. The system of claim 37, wherein Memory Recognition (MR) scans Chaotic Field to recognize known concepts, wherein the Chaotic Field is a 'field' of concepts arbitrarily

submersed in 'white noise' information, wherein Memory Concept Retention stores recognizable concepts that are ready to be indexed and referenced for field examination, wherein 3 Letter Scanner scans the Chaotic Field and checks against 3 letter segments that correspond to a target, wherein 5 Letter Scanner scans the Chaotic Field and checks against 5 letter segments that correspond to a target but this time the segment that is checked with every advancement throughout the field is the entire word, wherein the Chaotic field is segmented for scanning in different proportions, wherein as the scope of the scanning decreases, the accuracy increases, wherein as the field territory of the scanner increases, a larger letter scanner is more efficient for performing recognitions, at the expense of accuracy, wherein Memory Concept Indexing (MCI) alternates the size of the scanner in response to their being unprocessed memory concepts left, wherein MCI 500 starts with the largest available scanner and decreases gradually whereby more computing resources can be found to check for the potential existence of smaller memory concept targets.

41. The system of claim 37, wherein Field Interpretation Logic (FIL) operates the logistics for managing scanners of differing widths, wherein General Scope Scan begins with a large letter scan, and sifts through a large scope of field with fewer resources, at the expense of small scale accuracy, wherein Specific Scope Scan is used when an area of significance has been located, and needs to be 'zoomed in' on whereby ensuring that an expensively accurate scan isn't performed in a redundant and unyielding location, wherein receiving additional recognition of memory concepts in the Chaotic Field indicates that Field Scope contains a dense saturation of memory concepts.

42. The system of claim 37, wherein in Automated Perception Discovery Mechanism (APDM), Angle of Perceptions are defined in composition by multiple metrics including Scope, Type, Intensity and Consistency, which define multiple aspects of perception that compose the overall perception, wherein Creativity module produces complex variations of Perception, wherein the Perception Weight defines how much relative influence a Perception has whilst emulated by the POE, wherein the weights of both input Perceptions are considering whilst

defining the weight of the Newly Iterated Perception, which contains hybridized metrics that are influenced from the previous generation of Perceptions.

43. The system of claim 37, wherein input for the CVFG is Data Batch, which is an Arbitrary Collection of data that represents the data that must be represented by the node makeup of the generated CVF, wherein a sequential advancement is performed through each of the individual units defined by Data Batch, wherein the data unit is converted to a Node format, which has the same composition of information as referenced by the final CVF, wherein the converted Nodes are then temporarily stored in the Node Holdout upon checking for their existence at Stage, wherein if they are not found then they are created and updated with statistical information including occurrence and usage, wherein all the Nodes with the Holdout are assembled and pushed as modular output as a CVF.

44. The system of claim 37, wherein Node Comparison Algorithm compares two Node Makeups, which have been read from the raw CVF, wherein with Partial Match Mode (PMM), if there is an active node in one CVF and it is not found in its comparison candidate (the node is dormant), then the comparison is not penalized, wherein with Whole Match Mode WMM, If there is an active node in one CVF and it is not found in its comparison candidate (the node is dormant), then the comparison is penalized.

45. The system of claim 37, wherein System Metadata Separation (SMS) separates Input System Metadata into meaningful security cause-effect relationships, wherein with Subject Scan/Assimilation, the subject/suspect of a security situation is extracted from the system metadata using premade category containers and raw analysis from the Categorization Module, wherein the subject is used as the main reference point for deriving a security response/variable relationship, wherein with Risk Scan/Assimilation, the risk factors of a security situation are extracted from the system metadata using premade category containers and raw analysis from the Categorization Module, wherein the risk is associated with the target subject which exhibits or is exposed to such risk, wherein with Response Scan/Assimilation, the

response of a security situation made by the input algorithm is extracted from the system metadata using premade category containers and raw analysis from the Categorization Module, wherein the response is associated with the security subject which allegedly deserves such a response.

46. The system of claim 37, wherein in the MCM, Format Separation separates and categorizes the metadata is separated and categorized according to the rules and syntax of a recognized format, wherein Local Format Rules and Syntax contains the definitions that enable the MCM module to recognize pre-formatted streams of metadata, wherein Debugging Trace is a coding level trace that provides variables, functions, methods and classes that are used and their respective input and output variable type /content, wherein the Algorithm Trace is a Software level trace that provides security data coupled with algorithm analysis, wherein the resultant security decision (approve/block) is provided along with a trail of how it reached that decision (justification), and the appropriate weight that each factor contributed into making that security decision.

47. The system of claim 37, wherein in Metric Processing (MP), Security Response X represents a series of factors that contribute to the resultant security response chosen by the SPMA, wherein the initial weight is determined by the SPMA, wherein Perception Deduction (PD) uses a part of the security response and its corresponding system metadata to replicate the original perception of the security response, wherein Perception Interpretations of the Dimensional Series displays how PD will take the Security Response of the SPMA and associate the relevant Input System Metadata to recreate the full scope of the intelligent 'digital perception' as used originally by the SPMA, wherein Shape Fill, Stacking Quantity, and Dimensional are digital perceptions that capture the 'perspective' of an intelligent algorithm.

48. The system of claim 47, wherein in the PD, Security Response X is forwarded as input into Justification/Reasoning Calculation, which determines the justification of the security response of the SPMA by leveraging the intent supply of the Input/Output Reduction (IOR)

module, wherein the IOR module uses the separated input and output of the various function calls listed in the metadata, wherein the metadata separation is performed by the MCM.

49. The system of claim 37, wherein for the POE, Input System Metadata is the initial input that is used by Raw Perception Production (RP2) to produce perceptions in CVF, wherein with Storage Search (SS) the CVF derived from the data enhanced logs is used as criteria in a database lookup of the Perception Storage (PS), wherein in Ranking, the perceptions are ordered according to their final weight, wherein the Data Enhanced Logs are applied to the perceptions to produce block/approve recommendations, wherein the SCKD tags the logs to define the expected upper scope of unknown knowledge, wherein Data Parsing does a basic interpretation of the Data Enhanced Logs and the Input System Metadata to output the original Approve or Block Decision as decided by the original SPMA, wherein CTMP criticizes decisions in the POE according to perceptions, and in Rule Execution (RE) according to logically defined rules.

50. The system of claim 34, wherein with Metric Complexity, the outer bound of the circle represents the peak of known knowledge concerning the individual metric, wherein the outer edge of the circle represents more metric complexity, whilst the center represents less metric complexity, wherein the center light grey represents the metric combination of the current batch of Applied Angles of Perception, and the outer dark grey represents metric complexity that is stored and known by the system in general, wherein the goal of ID is to increase the complexity of relevant metrics, so that Angles of Perception can be multiplied in complexity and quantity, wherein the dark grey surface area represents the total scope of the current batch of Applied Angles of Perception, and the amount of scope left over according to the known upper bound, wherein upon enhancement and complexity enrichment the metrics are returned as Metric Complexity, which is passed as input of Metric Conversion, which reverses individual to whole Angles of Perception whereby the final output is assembled as Implied Angles of Perception.

51. The system of claim 37, wherein for SCKD, Known Data Categorization (KDC) categorically separates known information from Input so that an appropriate DB analogy query can be performed and separates the information into categories, wherein the separate categories individually provide input to the CVFG, which outputs the categorical information in CVF format, which is used by Storage Search (SS) to check for similarities in the Known Data Scope DB, wherein each category is tagged with its relevant scope of known data according to the SS results, wherein the tagged scopes of unknown information per category are reassembled back into the same stream of original input at the Unknown Data Combiner (UDC).

52. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Lexical Objectivity Mining (LOM), further comprising:

- a) Initial Query reasoning (IQR), to which a question is transferred, and which leverages Central Knowledge Retention (CKR) to decipher missing details that are crucial in understanding and answering/responding to the question;
- b) Survey Clarification (SC), to which the question and supplemental query data is transferred, and which receives input from and send output to human subject, and forms Clarified Question/Assertion;
- c) Assertion Construction (AC), which receives a proposition in a form of an assertion or question and provides output of concepts related to such proposition;
- d) Response Presentation, which is an interface for presenting a conclusion drawn by AC to both Human Subject and Rational Appeal (RA);
- e) Hierarchical Mapping (HM), which maps associated concepts to find corroboration or conflict in Question/Assertion consistency, and calculates benefits and risks of having a certain stance on the topic;

- f) Central Knowledge Retention (CKR), which is a main database for referencing knowledge for LOM;
- g) Knowledge Validation (KV), which receives high confidence and pre-criticized knowledge which needs to be logically separated for query capability and assimilation into the CKR;
- h) Accept Response, which is a choice given to the Human Subject to either accept a response of LOM or to appeal it with a criticism, wherein if the response is accepted, then it is processed by KV so that it can be stored in CKR as confirmed (high confidence) knowledge, wherein should the Human Subject not accept the response, they are forwarded to the RA, which checks and criticizes reasons of appeal given by Human;
- i) Managed Artificially Intelligent Services Provider (MAISP), which runs an internet cloud instance of LOM with a master instance of the CKR, and connects LOM to Front End Services, Back End Services, Third Party Application Dependencies, Information Sources, and the MNSP Cloud.

53. The system of claim 52, wherein Front End Services include Artificially Intelligent Personal Assistants, Communication Applications and Protocols, Home Automation and Medical Applications, wherein Back End Services include online shopping, online transportation, Medical Prescription ordering, wherein Front End and Back End Services interact with LOM via a documented API infrastructure, which enables standardization of information transfers and protocols, wherein LOM retrieves knowledge from external Information Sources via the Automated Research Mechanism (ARM).

54. The system of claim 53, wherein Linguistic Construction (LC) interprets raw question/assertion input from the Human Subject and parallel modules to produce a logical separation of linguistic syntax; wherein Concept Discovery (CD) receives points of interest within the Clarified Question/Assertion and derives associated concepts by leveraging CKR; wherein Concept Prioritization (CP) receives relevant concepts and orders them in logical tiers that represent specificity and generality; wherein Response Separation Logic (RSL) leverages the LC to understand the Human Response and associate a relevant and valid response with the

initial clarification request whereby accomplishing the objective of SC; wherein the LC is then re-leveraged during the output phase to amend the original Question/Assertion to include the supplemental information received by the SC; wherein Context Construction (CC) uses metadata from Assertion Construction (AC) and evidence from the Human subject to give raw facts to CTMP for critical thinking; wherein Decision Comparison (DC) determines the overlap between the pre-criticized and post-criticized decisions; wherein Concept Compatibility Detection (CCD) compares conceptual derivatives from the original Question/Assertion to ascertain the logical compatibility result; wherein Benefit/Risk Calculator (BRC) receives the compatibility results from the CCD and weighs the benefits and risks to form a uniform decision that encompasses the gradients of variables implicit in the concept makeup; wherein Concept Interaction (CI) assigns attributes that pertain to AC concepts to parts of the information collected from the Human Subject via Survey Clarification (SC).

55. The system of claim 54, wherein inside the IQR, LC receives the original Question /Assertion; the question is linguistically separated and IQR processes each individual word/phrase at a time leveraging the CKR; By referencing CKR, IQR considers the potential options that are possible considering the ambiguity of the word/phrase.

56. The system of claim 54, wherein Survey Clarification (SC) receives input from IQR, wherein the input contains series of Requested Clarifications that are to be answered by the Human Subject for an objective answer to the original Question/Assertion to be reached, wherein provided response to the clarifications are forwarded to Response Separation Logic (RSL), which correlates the responses with the clarification requests; wherein in parallel to the Requested Clarifications being processed, Clarification Linguistic Association is provided to LC, wherein the Association contains the internal relationship between Requested Clarifications and the language structure, which enables the RSL to amend the original Question/Assertion whereby LC outputs the Clarified Question.

57. The system of claim 54, wherein for Assertion Construction, which received the Clarified Question/Assertion, LC breaks the question down into Points of Interest, which are passed onto Concept Discovery, wherein CD derives associates concepts by leveraging CKR, wherein Concept Prioritization (CP) orders concepts into logical tiers, wherein the top tier is assigned the most general concepts, whilst the lower tiers are allocated increasingly specific concepts, wherein the top tier is transferred to Hierarchical Mapping (HM) as modular input, wherein in a parallel transfer of information HM receives the Points of Interest, which are processed by its dependency module Concept Interaction (CI), wherein CI assigns attributes to the Points of Interest by accessing the indexed information at CKR, wherein upon HM completing its internal process, its final output is returned to AC after the derived concepts have been tested for compatibility and the benefits/risks of a stance are weighed and returned.

58. The system of claim 57, wherein for HM, CI provides input to CCD which discerns the compatibility/conflict level between two concepts, wherein the compatibility/conflict data is forwarded to BRC, which translates the compatibilities and conflicts into benefits and risks concerning taking a holistic uniform stance on the issue, wherein the stances, along with their risk/benefit factors, are forwarded to AC as Modular Output, wherein the system contains loops of information flow indicates gradients of intelligence being gradually supplemented as the subjective nature of the question/assertion a gradually built objective response; wherein CI receives Points of Interest and interprets each one according to the top tier of prioritized concepts.

59. The system of claim 54, wherein for RA, Core Logic processes the converted linguistic text, and returns result, wherein if the Result is High Confidence, the result is passed onto Knowledge Validation (KV) for proper assimilation into CKR, wherein if the Result is Low Confidence, the result is passed onto AC to continue the cycle of self-criticism, wherein Core Logic receives input from LC in the form of a Pre-Criticized Decision without linguistic elements, wherein the Decision is forwarded to CTMP as the Subjective Opinion, wherein Decision is also forwarded to Context Construction (CC) which uses metadata from AC and potential evidence

from the Human Subject to give raw facts to CTMP as input 'Objective Fact', wherein with CTMP having received its two mandatory inputs, such information is processed to output it's best attempt of reaching 'Objective Opinion,' wherein the opinion is treated internally within RA as the Post-Criticized Decision, wherein both Pre-Criticized and Post-Criticized decisions are forwarded to Decision Comparison (DC), which determines the scope of overlap between both decisions, wherein the appeal argument is then either conceded as true or the counter-point is improved to explain why the appeal is invalid, wherein indifferent to a Concede or Improve scenario, a result of high confidence is passed onto KV and a result of low confidence is passed onto AC 808 for further analysis.

60. The system of claim 54, wherein for CKR, units of information are stored in the Unit Knowledge Format (UKF), wherein Rule Syntax Format (RSF) is a set of syntactical standards for keeping track of references rules, wherein multiple units of rules within the RSF can be leveraged to describe a single object or action; wherein Source attribution is a collection of complex data that keeps track of claimed sources of information, wherein a UKF Cluster is composed of a chain of UKF variants linked to define jurisdictionally separate information, wherein UKF2 contains the main targeted information, wherein UKF1 contains Timestamp information and hence omits the timestamp field itself to avoid an infinite regress, wherein UKF3 contains Source Attribution information and hence omits the source field itself to avoid an infinite regress; wherein every UKF2 must be accompanied by at least one UKF1 and one UKF3, or else the cluster (sequence) is considered incomplete and the information therein cannot be processed yet by LOM Systemwide General Logic; wherein in between the central UKF2 and its corresponding UKF1 and UKF3 units there can be UKF2 units that act as a linked bridge, wherein a series of UKF Clusters will be processed by KCA to form Derived Assertion, wherein Knowledge Corroboration Analysis (KCA) is where UKF Clustered information is compared for corroborating evidence concerning an opinionated stance, wherein after processing of KCA is complete, CKR can output a concluded Opinionated stance on a topic.

61. The system of claim 54, wherein for ARM, wherein as indicated by User Activity, as users interact with LOM concepts are either directly or indirectly brought as relevant to answering/responding to a question/assertion, wherein User Activity is expected to eventually yield concepts that CKR has low or no information regarding, as indicated by List of Requested Yet Unavailable Concepts, wherein with Concept Sorting & Prioritization (CSP), Concept definitions are received from three independent sources and are aggregated to prioritize the resources of Information Request, wherein the data provided by the information sources are received and parsed at Information Aggregator (IA) according to what concept definition requested them and relevant meta-data are kept, wherein the information is sent to Cross-Reference Analysis (CRA) where the information received is compared to and constructed considering pre-existing knowledge from CKR.

62. The system of claim 54, wherein Personal Intelligence Profile (PIP) is where an individual's personal information is stored via multiple potential end-points and front-ends, wherein their information is isolated from CKR, yet is available for LOM Systemwide General Logic, wherein Personal information relating to Artificial Intelligence applications are encrypted and stored in the Personal UKF Cluster Pool in UKF format, wherein with Information Anonymization Process (IAP) information is supplemented to CKR after being stripped of any personally identifiable information, wherein with Cross-Reference Analysis (CRA) information received is compared to and constructed considering pre-existing knowledge from CKR.

63. The system of claim 54, wherein Life Administration & Automation (LAA) connects internet enabled devices and services on a cohesive platform, wherein Active Decision Making (ADM) considers the availability and functionality of Front End Services, Back End Services, IoT devices, spending rules and amount available according to Fund Appropriations Rules & Management (FARM); FARM receives human input defining criteria, limits and scope to the module to inform ADM for what it's jurisdiction of activity is, wherein cryptocurrency funds is deposited into the Digital Wallet, wherein the IoT Interaction Module (IIM) maintains a

database of what IoT devices are available, wherein Data Feeds represents when IoT enabled devices send information to LAA.

64. The system of claim 52, further comprising Behavior Monitoring (BM) which monitors personally identifiable data requests from users to check for unethical and/or illegal material, wherein with Metadata Aggregation (MDA) user related data is aggregated from external services so that the digital identity of the user can be established, wherein such information is transferred to Induction/Deduction, and eventually PCD, where a sophisticated analysis is performed with corroborating factors from the MNSP; wherein all information from the authenticated user that is destined for PIP passes through Information Tracking (IT) and is checked against the Behavior Blacklist, wherein at Pre-Crime Detection (PCD) Deduction and Induction information is merged and analyzed for pre-crime conclusions, wherein PCD makes use of CTMP, which directly references the Behavior Blacklist to verify the stances produced by Induction and Deduction, wherein the Blacklist Maintenance Authority (BMA) operates within the Cloud Service Framework of MNSP.

65. The system of claim 63, wherein LOM is configured to manage a personalized portfolio on an individual's life, wherein LOM receives an initial Question which leads to conclusion via LOM's Internal Deliberation Process, wherein it is connected to connect to the LAA module which connects to internet enabled devices which LOM can receive data from and control, wherein with Contextualization LOM deduces the missing links in constructing an argument, wherein LOM has deciphers with its logic that to solve the dilemma posed by the original assertion it must first know or assume certain variables about the situation.

66. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein

the computer implemented system is Linear Atomic Quantum Information Transfer (LAQIT), comprising:

a) recursively repeating same consistent color sequence within a logically structured syntax; and

b) using a sequence recursively to translate with the English alphabet;

wherein when structuring a 'base' layer of the English alphabet, the color sequence is used with a shortened and unequal weight on a color channel and leftover space for syntax definitions within the color channel is reserved for future use and expansion;

wherein a complex algorithm reports its log events and status reports with LAQIT, status/log reports are automatically generated, wherein the status/log reports are converted to a transportable text-based LAQIT syntax, wherein syntactically insecure information is transferred over digitally, wherein a transportable text-based syntax is converted to highly readable LAQIT visual syntax (linear mode), wherein Key is optimized for human memorization and is based on relatively short sequence of shapes;

wherein locally non-secure text is entered by a sender for submission to a Recipient, wherein a text is converted to a transportable encrypted text-based LAQIT syntax, wherein syntactically secure information is transferred over digitally, wherein data is converted to a visually encrypted LAQIT syntax;

wherein Incremental Recognition Effect (IRE) is a channel of information transfer, and recognizes a full form of a unit of information before it has been fully delivered, wherein this effect of a predictive index is incorporated by displaying transitions between word to word, wherein Proximal Recognition Effect (PRE) is a channel of information transfer, and recognizes the full form of a unit of information whilst it is either corrupted, mixed up or changed.

67. The system of claim 66, wherein in the Linear mode of LAQIT, a Block shows the 'Basic Rendering' version of linear mode and a Point displays its absence of encryption, wherein with Word Separator, the color of the shape represents the character that follows the word and acts as a separation between it and the next word, wherein Single Viewing Zone incorporates a smaller viewing zone with larger letters and hence less information per pixel, wherein in Double

Viewing Zone, there are more active letters per pixel, wherein Shade Cover makes incoming and outgoing letters dull so that the primary focus of the observer is on the viewing zone.

68. The system of claim 66, wherein in Atomic Mode, which is capable of a wide range of encryption levels, the Base main character reference will specify the general of which letter is being defined, wherein a Kicker exists with the same color range as the bases, and defines the specific character exactly, wherein with Reading Direction, the information delivery reading begins on the top square of orbital ring one, wherein once an orbital ring has been completed, reading continues from the top square of the next sequential orbital ring, wherein the Entry/Exit Portals are the points of creation and destruction of a character (its base), wherein a new character, belonging to the relevant orbital, will emerge from the portal and slide to its position clockwise, wherein the Atomic Nucleus defines the character that follows the word; wherein with Word Navigation, each block represents an entire word (or multiple words in molecular mode) on the left side of the screen, wherein when a word is displayed, the respective block moves outwards to the right, and when that word is complete the block retreats back, wherein the color/shape of the navigation block is the same color/shape as the base of the first letter of the word; wherein with Sentence Navigation, each block represents a cluster of words, wherein a cluster is the maximum amount of words that can fit on the word navigation pane; wherein Atomic State Creation is a transition that induces the Incremental Recognition Effect (IRE), wherein with such a transition Bases emerge from the Entry/Exit Portals, with their Kickers hidden, and move clockwise to assume their positions.; wherein Atomic State Expansion is a transition that induces the Proximal Recognition Effect (PRE), wherein once the Bases have reached their position, they move outwards in the 'expand' sequence of the information state presentation, which reveals the Kickers whereby the specific definition of the information state can be presented; wherein Atomic State Destruction is a transition that induces the Incremental Recognition Effect (IRE), wherein Bases have retracted, (reversed the Expansion Sequence) to cover the Kickers again, wherein they are now sliding clockwise to reach the entry/exit portal.

69. The system of claim 68, wherein with Shape Obfuscation, the standard squares are replaced with five visually distinct shapes, wherein the variance of shapes within the syntax allows for dud (fake) letters to be inserted at strategic points of the atomic profile and the dud letters obfuscate the true and intended meaning of the message, wherein deciphering whether a letter is real or a dud is done via the securely and temporarily transferred decryption key;

wherein with Redirection Bonds, a bond connects two letters together and alters the flow of reading, wherein whilst beginning with the typical clockwise reading pattern, encountering a bond that launches (starts with) and lands on (ends with) legitimate/non-dud letters will divert the reading pattern to resume on the landing letter;

wherein with Radioactive Elements, some elements can 'rattle' which can inverse the evaluation of if a letter is a dud or not, wherein Shapes shows the shapes available for encryption, wherein Center Elements shows the center element of the orbital which defines the character that comes immediately after the word.

70. The system of claim 69, wherein with Redirection Bonds, the bonds start on a 'launching' letter and end on a 'landing' letter, either of which may or may not be a dud, wherein if none of them are duds, then the bond alters the reading direction and position, wherein If one or both are duds, then the entire bond must be ignored, or else the message will be decrypted incorrectly, wherein with Bond Key Definition, if a bond must be followed in the reading of the informations state depends on if it has been specifically defined in the encryption key.

71. The system of claim 69, wherein with Single Cluster, both neighbors are non-radioactive, hence the scope for the cluster is defined, wherein since the key specifies double clusters as being valid, the element is to be treated is if it wasn't radioactive in the first place, wherein with Double Cluster, Key Definition defines double clusters as being active, hence all other sized clusters are to be considered dormant whilst decrypting the message, wherein Incorrect Interpretation shows how the interpreter did not treat the Double Cluster as a reversed sequence (false positive).

72. The system of claim 69, wherein in Molecular Mode with Encryption and Streaming enabled, with Covert Dictionary Attack Resistance, an incorrect decryption of the message leads to a 'red herring' alternate message, wherein with Multiple Active Words per Molecule, the words are presented in parallel during the molecular procedure whereby increasing the information per surface area ratio, however with a consistent transition speed, wherein Binary and Streaming Mode shows Streaming Mode whilst in a typical atomic configuration the reading mode is Binary, wherein Binary Mode indicates that the center element defines which character follows the word, wherein Molecular mode is also binary; except when encryption is enabled which adheres to Streaming mode, wherein Streaming mode makes references within the orbital to special characters.

73. A COMPUTER SECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE, wherein the system having a memory that stores programmed instructions, a processor that is coupled to the memory and executes the programmed instructions and at least one database, wherein the system comprising a computer implemented system of providing designated functions, wherein the computer implemented system is Universal BCHAIN Everything Connections (UBEC) system with Base Connection Harmonization Attaching Integrated Nodes, further comprising:

- a) Communications Gateway (CG), which is a primary algorithm for BCHAIN Node to interact with its Hardware Interface thereafter leading to communications with other BCHAIN nodes;
- b) Node Statistical Survey (NSS), which interprets remote node behavior patterns;
- c) Node Escape Index, which tracks a likelihood that a node neighbor will escape a perceiving node's vicinity;
- d) Node Saturation Index, which tracks an amount of nodes in a perceiving node's range of detection;
- e) Node Consistency Index, which tracks a quality of nodes services as interpreted by a perceiving node, wherein a high Node Consistency Index indicates that surrounding neighbor nodes tend to have more availability uptime and consistency in performance, wherein nodes

that have dual purposes in usage tend to have a lower Consistency Index, wherein nodes that are dedicated to the BCHAIN network exhibit a higher value; and

f) Node Overlap Index, which tracks an amount of overlap nodes have with one another as interpreted by a perceiving node.

74. The system of claim 73, further comprising:

a) Customchain Recognition Module (CRM), which connects with Customchains including Appchains or Microchains that have been previously registered by the node, wherein CRM informs the rest of the BCHAIN Protocol when an update has been detected on an Appchain's section in the Metachain or a Microchain's Metachain Emulator;

b) Content Claim Delivery (CCD), which receives a validated CCR and thereafter sends the relevant CCF to fulfill the request;

c) Dynamic Strategy Adaptation (DSA), which manages the Strategy Creation Module (SCM), which dynamically generates a new Strategy Deployment by using the Creativity Module to hybridize complex strategies that have been preferred by the system via Optimized Strategy Selection Algorithm (OSSA), wherein New Strategies are varied according to input provided by Field Chaos Interpretation;

d) Cryptographic Digital Economic Exchange (CDEE) with a variety of Economic Personalities managed by the Graphical User Interface (GUI) under the UBEC Platform Interface (UPI); wherein with Personality A, Node resources are consumed to only match what you consume, wherein Personality B Consumes as many resources as possible as long as the profit margin is greater than predetermined value, wherein Personality C pays for work units via a traded currency, wherein with Personality D Node resources are spent as much as possible and without any restriction of expecting anything in return, whether that be the consumption of content or monetary compensation;

e) Current Work Status Interpretation (CWSI), which References the Infrastructure Economy section of the Metachain to determine the current surplus or deficit of this node with regards to work done credit;

- f) Economically Considered Work Imposition (ECWI), which considers the selected Economic Personality with the Current Work Surplus/Deficit to evaluate if more work should currently be performed; and
- g) Symbiotic Recursive Intelligence Advancement (SRIA), which is a triad relationship between different algorithms comprising LIZARD, which improves an algorithm's source code by understanding code purpose, including itself, I2GE, which emulates generations of virtual program iterations, and the BCHAIN network, which is a vast network of chaotically connected nodes that can run complex data-heavy programs in a decentralized manner.