Prototype Orchestration Framework as a High Exposure Dimension Cyber Defense Accelerant Amidst Ever-Increasing Cycles of Adaptation by Attackers

A Modified Deep Belief Network Accelerated by a Stacked Generative Adversarial Network for Enhanced Event Correlation

Steve Chan
Decision Engineering Analysis Laboratory
San Diego, California U.S.A.
email: schan@dengineering.org

Abstract—**The cycles of adaptation by attackers are ever-increasing. To meet these evolving threats, outsourcing to Managed Security Service Providers (MSSPs) has become prevalent. As these MSSPs contend with a torrent of varied attack vectors, they are increasingly utilizing Artificial Intelligence (AI) to assist them in protecting their clients. Practitioners often assert that systems which provide decisions can be construed as AI; along this vein, this paper presents summary results of a prototype orchestration framework that selects and prioritizes cyber tools to be utilized against a continuous stream of testbed cyber-attacks. This orchestration framework is predicated upon the hybridization of a modified Deep Belief Network (DBN) conjoined with a particular cognitive computing precept (the acceptance of higher uncertainty amidst lower ambiguity for compressed decision cycles); for uncompressed decision cycles, it utilizes a modified Stacked Generative Adversarial Network (SGAN), which serves as a feeder to a Lowering Ambiguity Accelerant (LAA). Results show promise during the 1-5 day period; work has already commenced for improving the performance for day 6+, and uptime is already at 38 days with minimal degradation.**

Keywords-Cyber Attack Accelerants; Orchestration Framework; Uncertainty/Ambiguity Calculus; Deep Belief Network; Generative Adversarial Network.

I. INTRODUCTION

Organizations in the Indo-Asia Pacific are currently undergoing a rapid phase of Information Technology (IT) development. Yet, with a large number of companies belonging to the Small and Medium Enterprises (SMEs) segment, there is limited capital available for massive investment into IT infrastructures and manpower. This has resulted in these SMEs (and large industries alike) to turn to third-party Managed Service Providers (MSPs), who can handle the maintenance and monitoring of their mission-critical applications around the clock. This operational tempo for the MSPs has necessitated the use of Artificial Intelligence (AI) to consolidate data and streamline processes in their continuous efforts to defend both SMEs and enterprise level companies. This paper presents a modified Stacked Generative Adversarial Network (SGAN) for uncompressed decision cycles and a modified Deep Belief Network (DBN) for compressed decision cycles. A particular focus is given to the AI accelerant methodology utilized to compress the decision-making cycles of the prototype orchestration framework.

The remainder of this paper is organized as follows: Section II discusses the ecosystem of managed service providers and managed security service providers as well as an exemplar sector (e.g. energy). Subsequently, Section III explores potential accelerants for cyber attackers, which ironically also serve as instruments for cyber defenders. Then, Section IV delves into a posited prototype orchestration framework to help mitigate against accelerated cyber-attacks. Section V posits a cognitive computing precept (e.g. tolerance for higher uncertainty); of note, Section V also provides pertinent background context regarding precision/accuracy and quantitative/qualitative data. The inclusion of Section VA and VB should be clarified. Prodigious amounts of funding have been spent on biomimetic projects, such as attempting to emulate the brain, via synthetic processes. However, in the emulation, oftentimes, certain vital aspects are excluded during the dimensionality reduction of the problem. Indeed, many projects have suffered as they have missed the criticality of the inclusion of certain dimensions, such as morphology. To articulate this "lessons learned" vantage point, this paper focuses upon the underlying logic needed to inform future biomimetic efforts. Section VI posits an artificial intelligence precept (e.g. desire for gestaltian closure); of note, Section VI also provides pertinent background context regarding deeper belief amidst compressed decision cycles, the use of a deep belief network over deep learning amidst compressed decision cycles, and a higher tolerance for uncertainty amidst compressed decision cycles. Furthermore, the topics of Section VI are expounded upon because the hybridization of artificial intelligence precepts with cognitive computing precepts for machine-speed performance is often not treated synchronously. In fact, many projects claim accelerated performance, but often do not incorporate a Deep Belief component for handling decision-making amidst compressed decision cycles. Avoiding the challenge of these trans-disciplinary issues often results in only incremental improvement paradigms. Section VII presents the experimental results from the hybridized computational methodology of Section V and Section VI. Section VIII presents further enhancements to the posited hybridized computational methodology of Section VII. Finally, the paper reviews and emphasizes key points within Section IX, the conclusion.

II. Ecosystem of Managed Service Providers

A. Managed Service Providers (MSPs)

MSPs are, in many cases, an IT services provider that manages a defined set of services for its clients, as agreed prior, or as the MSP (in many cases, not the client) proactively determines. MSP roles have evolved as they have gone from simply maintaining legacy systems (a report by Cisco posits that 65% of IT budgets are allocated for keeping systems functional [1]). In contemporary times, the MSP remotely manages the client's IT infrastructure and/or end-user systems, typically under a subscription model or "pay as you go" pricing model. According to MarketsandMarkets, the global MSP market is forecast to grow from USD$107.17 billion in 2014 to USD$193.34 billion by 2019 [2], and the market is expected to increase as more clients are focusing on their core competencies rather than on IT maintenance and troubleshooting issues. The current compound annual growth rate (CAGR) is 12.5% [2], and this CAGR is expected to rise quickly as IT expenditures shift from a capital expenditure (CapEx) to operational expenditure (OpEx) model.

B. Managed Security Service Providers (MSSPs)

MSP responsibilities are increasingly shifting from repairs, patches, delivery of new software, and incorporation of cloud services to that of data-related security services. According to Gartner, a new class of MSP, the Managed Security Service Provider (MSSP), has emerged to provide outsourced monitoring and management of security devices and systems. Prototypical managed services now include, among others, managed firewall, virtual private network, vulnerability scanning, anti-viral services, and intrusion detection. Outsourcing to MSSPs has typically improved the client ability to deter cyberthreats, and among other assessments, the *Gartner Magic Quadrant (MQ) for Managed Security Service Providers* and the *International Data Corporation (IDC) MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment* compares and contrasts MSSPs. MSSPs have burgeoned not only in industries that have experienced massive compromises in recent times (e.g., healthcare), but also in areas that are at unprecedented levels of risk (e.g., energy sector).

C. MSPs and MSSPs for the Energy Sector

By leveraging available high-speed Internet connections and user-friendly Software-as-a-Service (SAAS) interfaces, MSPs within the energy sector are helping building owners and operators lower energy usage, increase building operations efficiency, and optimize the climate control conditions in tenant working spaces. These MSPs are endeavoring to leverage cloud-based software and the more granular control of Internet of Things (IOT) devices to deliver their managed services. This paradigm has yielded new vulnerabilities within the cyber domain, such as in Figure 1.

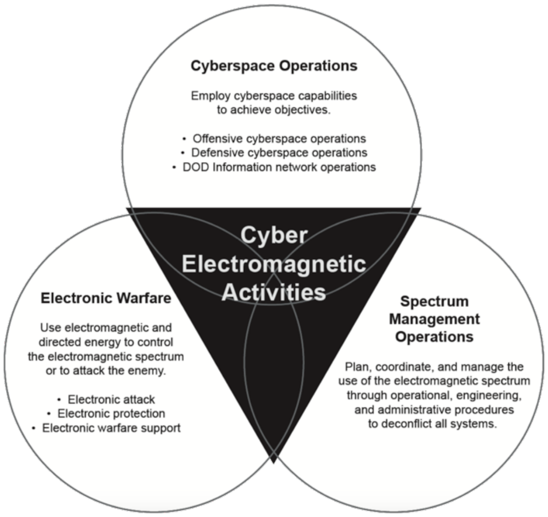

Cyberspace Operations
Employ cyberspace capabilities to achieve objectives.
• Offensive cyberspace operations
• Defensive cyberspace operations
• DOD Information network operations
Cyber Electromagnetic Activities
Electronic Warfare
Use electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.
• Electronic attack
• Electronic protection
• Electronic warfare support
Spectrum Management Operations
Plan, coordinate, and manage the use of the electromagnetic spectrum through operational, engineering, and administrative procedures to deconflict all systems.

Figure 1. Cyber Electromagnetic Vulnerabilities [3].

MSSPs, such as within the energy sector, are scrutinizing the attack surface problem — the exposure or exploitable vulnerabilities that exist within a system — particularly at the "weak links in the chain" (which represents the weakest members of a system, and because of these points of failure, the entire system may fail). It is well known that the three most common attack surfaces include: (1) human attack surface (e.g., social engineering, insider threat, errors of omission or commission), (2) network attack surface (e.g., open ports on outward-facing Web servers, code listening on those ports, and services available on the inside of the firewall), and (3) software attack surface (with a focus on Web applications).

Putting aside the large issue of human attack surfaces, the SANS Technology Institute asserts that the amalgam of network attack surfaces and software attack surfaces constitute high exposure dimensions. With regards to software attack surfaces, an ever-increasing amount of funding is being spent on developing an escalating number of Web applications that are mission-critical. Concurrently, attackers are becoming more adept at exploiting Web applications. There is a plethora of penetration testing (a.k.a. pen testing) tools and Web application security assessment tools that help identify known and unknown vulnerabilities. These tools can assist in: (1) reducing the amount of code executing (i.e. turning off certain features), (2) reducing the volume of code that is accessible to users (i.e. establishing user privileges), (3) constraining the damage, if code is indeed exploited (i.e. damage control rule sets). However, there are limitations to these prototypical tools. Pen testing itself is limited in scope, and most organizations are not able to exhaustively test the entire portfolio of their systems due to resource constraints and practicality. Also, as pen testing involves a particular set of tests over a certain amount of time, attackers can plan and execute over a longer time frame. Furthermore, pen testing is limited to the models that are created, and the attack surface might be at higher exposure than anticipated. There are also limitations to the automated tools for Web application security scanning. While scanners can identify the more serious technical flaws within applications, they are not able to identify logical (e.g., architectural, design) flaws that were introduced before the coding, authentication, and authorization took place.

III. Accelerants for Cyber Attackers

Cyber attackers are becoming increasingly adept. Just as MSPs and MSSPs are leveraging early warning indicators, such as the National Vulnerability Database (NVD) and Sentient Hyper Optimized Data Access Network (SHODAN), cyber attackers are also leveraging these assets for exploitation opportunities and as attack accelerants.

A. NVD

The National Institute of Standards and Technology's (NIST) NVD lists various known vulnerabilities. The NVD utilizes a Common Vulnerability Scoring System (CVSS), which provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. A sample vulnerability and CVSS score is shown in Table 1.

TABLE 1. CHARACTERISTICS OF A NATIONAL VULNERABILITY DATABASE (NVD) VULNERABILITY

Characteristics of an NVD Vulnerability	Description
CVSS 2.0 Base Score	***High*** 7.8
Vulnerability Type(s)	Denial of Service
Availability Impact	***Complete*** (there is a total shutdown of the affected resource. The attacker can render the resource completely unavailable).
Access Complexity	***Low*** (specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit).
Authentication	***Not required*** (authentication is not required to exploit the vulnerability).

The NVD's CVSS Specification Documents provide severity explanations. For this example, a CVSS Base Score of 7.8 is high, whether it is for the CVSS v2.0 Specification Document or for the CVSS v3.0 Specification Document, as is articulated (bolded and italicized) in Table 2 and Table 3.

TABLE 2. CVSS V2.0 RATINGS

Severity	Base Score Range
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	***7.0 – 10.0***

TABLE 3. CVSS V3.0 RATINGS

Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	***7.0 - 8.9***
Critical	9.0 - 10.0

B. SHODAN

Unlike traditional search engines that obtain information on the World Wide Web (WWW), SHODAN endeavors to obtain data from the ports of Internet-connected devices accessible by the WWW. Hence, cyber attackers can exploit SHODAN to find various technologies including the Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS) of the energy sector. Attackers can accelerate their attack by performing bulk searching and processing of SHODAN queries, via software called SHODAN Diggity, which provides a list of 167 search queries in a dictionary file, known as the SHODAN Hacking Database (SHDB). The described process, as shown in Figure 2, is streamlined and enhanced by SearchDiggity, which is a Graphical User Interface (GUI) application developed for the Google Hacking Diggity Project. It serves as a front-end to SHODAN Diggity. In essence, an attack surface area may be at greater exposure due to the combinatorial of elements (e.g., Search Diggity, SHODAN, SHODAN Diggity, SHDB, etc.) that may be utilized maliciously by an attacker as accelerants.

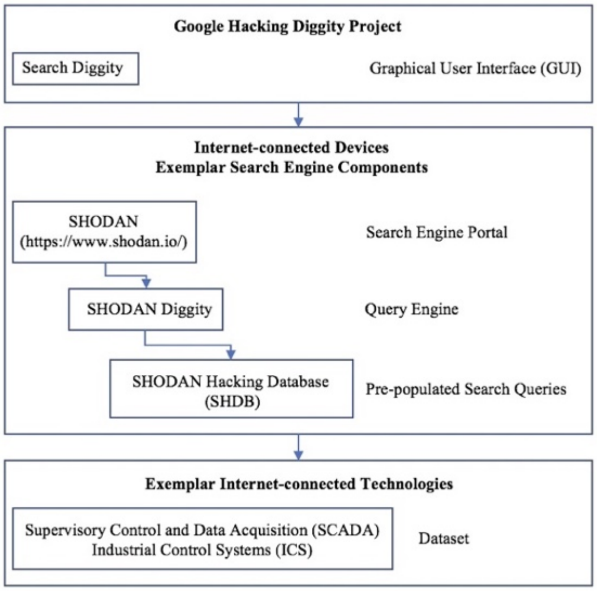

Google Hacking Diggity Project
Search Diggity
Graphical User Interface (GUI)
Internet-connected Devices
Exemplar Search Engine Components
SHODAN
(https://www.shodan.io/)
Search Engine Portal
SHODAN Diggity
Query Engine
SHODAN Hacking Database
(SHDB)
Pre-populated Search Queries
Exemplar Internet-connected Technologies
Supervisory Control and Data Acquisition (SCADA)
Industrial Control Systems (ICS)
Dataset

Figure 2. Interplay among the Components of an Internet-connected Devices Search Engine and Exemplar Internet-connected Technologies.

There are many other potential attack accelerants in addition to SHODAN.

IV. A PROTOTYPE ORCHESTRATION FRAMEWORK TO MITIGATE AGAINST ACCELERATED CYBER ATTACKS

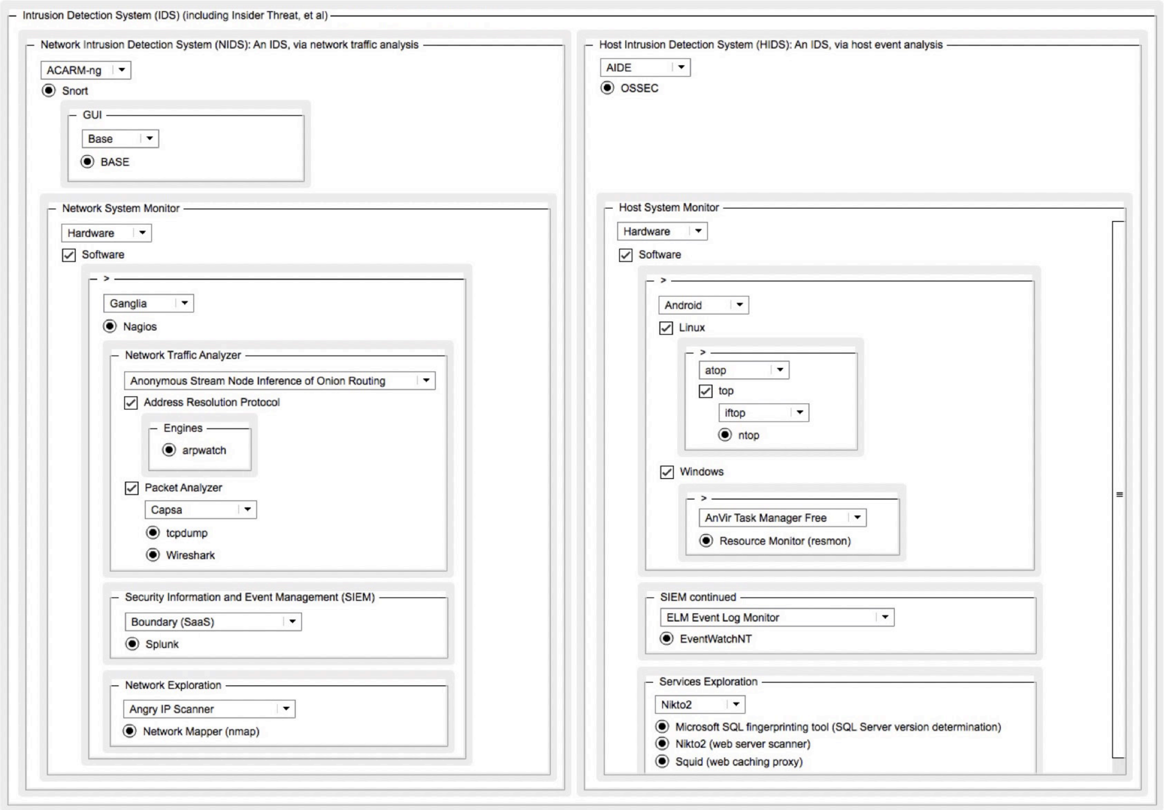
As MSPs and MSSPs are determining the services that are needed by their clients, particularly within the energy sector, they are increasingly prototyping various cyber defense frameworks and tools. According to MSP Alliance (an international association of cloud computing providers and MSPs) contributor Charles Weaver, "the most advanced tools become feathers in the caps of service providers" [4].

This paper focused upon a research project that involved devising a prototype orchestration framework, which focused upon Intrusion Detection Systems (IDS) (a security technology originally built for detecting vulnerability exploits), Network Intrusion Detection Systems (NIDS) (a device or software application that monitors a network of systems), Host Intrusion Detection System (HIDS) (a system of monitoring and analyzing the internals of a computing system, as well as the network packets at its network interfaces), Network System Monitors (NSM) (a system that constantly monitors a network for slow or failing components, and in many cases, an assigned tool(s) will try to recover the problem by running a system administrator-defined program or by restarting a process), and Host System Monitors (HSM) (a more localized non-network monitoring agent). This is delineated in Figure 3. Within this figure, various Off-the-Shelf (OTS) tools are organized under IDS. Some of the presented tools include the following.

- *Snort.* Free, open source NIDS software. Entered InfoWorld's Open Source Hall of Fame as one of the "greatest open source software of all time" [5];
- *OSSEC.* Free, open source HIDS software;
- *Wireshark.* Free, open source NSM packet analyzer. Acclaimed by IDG Research as the "world's leading network traffic analyzer" [6];
- *Server Health Monitor.* Free HSM software.

The tools are further organized as follows: (1) NIDS (with NSM sub-category), and (2) HIDS (with HSM sub-category) categories. For example, "Snort" is categorized under NIDS, "OSSEC" under HIDS, "Wireshark" under NSM, and "Server Health Monitor" under HSM.

The discussed prototype orchestration framework does indeed endeavor to recognize the type of cyber-attack, but the focus is on how it procedurally recommends certain tools to be run against the attack vector (refer to Figure 4), recommends accelerant tools (third-party enhancements) based upon the decision cycles available (please refer to Figure 5), and further recommends tools based upon the effectiveness of the prior tools utilized (please refer to Figure 6). In essence, the involved prototype orchestration framework is predicated upon the hybridized computational methodology discussed herein.


Intrusion Detection System (IDS) (including Insider Threat, et al)

Network Intrusion Detection System (NIDS): An IDS, via network traffic analysis
ACARM-ng ▾
● Snort
GUI
Base ▾
● BASE
Network System Monitor
Hardware ▾
☑ Software
>
Ganglia ▾
● Nagios
Network Traffic Analyzer
Anonymous Stream Node Inference of Onion Routing ▾
☑ Address Resolution Protocol
Engines
● arpwatch
☑ Packet Analyzer
Capsa ▾
● tcpdump
● Wireshark
Security Information and Event Management (SIEM)
Boundary (SaaS) ▾
● Splunk
Network Exploration
Angry IP Scanner ▾
● Network Mapper (nmap)

Host Intrusion Detection System (HIDS): An IDS, via host event analysis
AIDE ▾
● OSSEC
Host System Monitor
Hardware ▾
☑ Software
>
Android ▾
☑ Linux
>
atop ▾
☑ top
iftop ▾
● ntop
☑ Windows
>
AnVir Task Manager Free ▾
● Resource Monitor (resmon)
SIEM continued
ELM Event Log Monitor ▾
● EventWatchNT
Services Exploration
Nikto2 ▾
● Microsoft SQL fingerprinting tool (SQL Server version determination)
● Nikto2 (web server scanner)
● Squid (web caching proxy)

Figure 3. Prototype Orchestration Framework for IDS: NIDS (with NSM) & HIDS (with HSM).

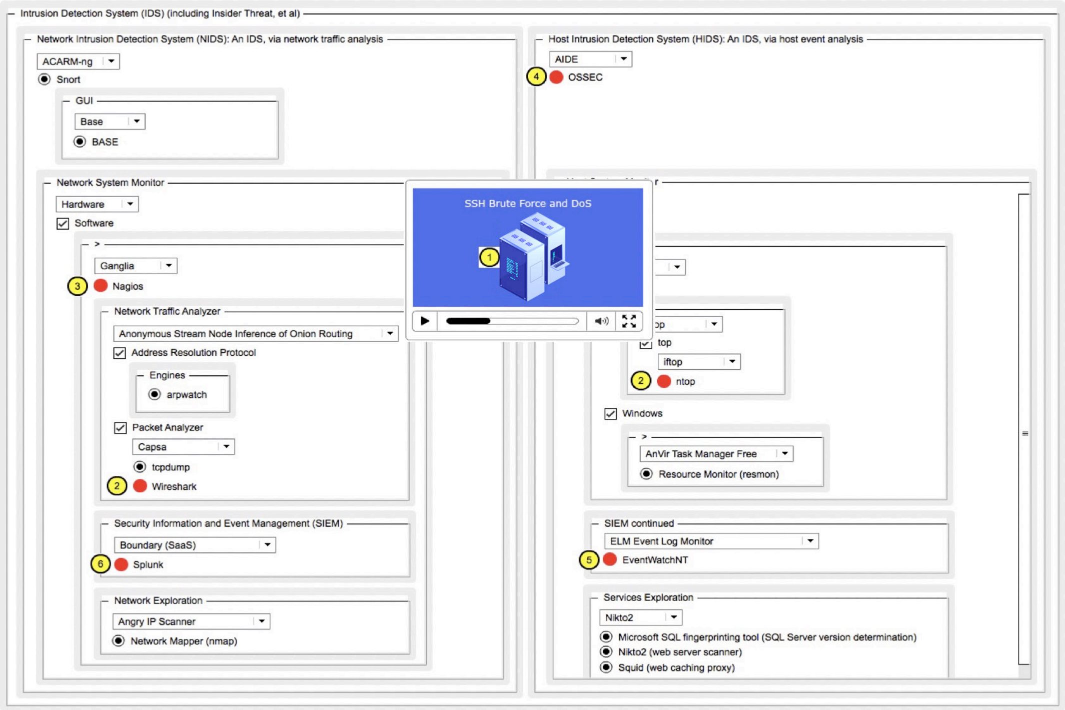

Intrusion Detection System (IDS) (including Insider Threat, et al)
Network Intrusion Detection System (NIDS): An IDS, via network traffic analysis
ACARM-ng
Snort
GUI
Base
BASE
Network System Monitor
Hardware
Software
Ganglia
3
Nagios
Network Traffic Analyzer
Anonymous Stream Node Inference of Onion Routing
Address Resolution Protocol
Engines
arpwatch
Packet Analyzer
Capsa
tcpdump
2
Wireshark
Security Information and Event Management (SIEM)
Boundary (SaaS)
6
Splunk
Network Exploration
Angry IP Scanner
Network Mapper (nmap)
Host Intrusion Detection System (HIDS): An IDS, via host event analysis
AIDE
4
OSSEC
SSH Brute Force and DoS
1
top
iftop
2
ntop
Windows
AnVir Task Manager Free
Resource Monitor (resmon)
SIEM continued
ELM Event Log Monitor
5
EventWatchNT
Services Exploration
Nikto2
Microsoft SQL fingerprinting tool (SQL Server version determination)
Nikto2 (web server scanner)
Squid (web caching proxy)

Figure 4. Prototype Orchestration Framework identifies the attack vector (e.g., Secure Socket Shell [SSH] Brute Force as well as Denial-of-Service [DoS]) and procedurally recommends certain tools.

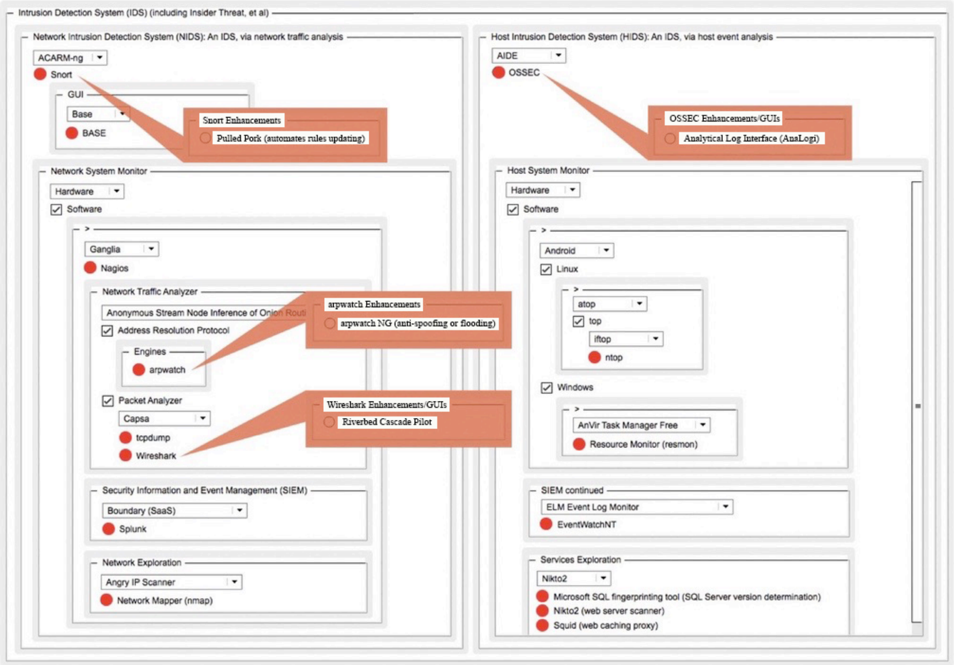

Intrusion Detection System (IDS) (including Insider Threat, et al)
Network Intrusion Detection System (NIDS): An IDS, via network traffic analysis
ACARM-ng
Snort
GUI
Base
BASE
Snort Enhancements
Pulled Pork (automates rules updating)
Network System Monitor
Hardware
Software
Ganglia
Nagios
Network Traffic Analyzer
Anonymous Stream Node Inference of Onion Routi
Address Resolution Protocol
Engines
arpwatch
arpwatch Enhancements
arpwatch NG (anti-spoofing or flooding)
Packet Analyzer
Capsa
tcpdump
Wireshark
Wireshark Enhancements/GUIs
Riverbed Cascade Pilot
Security Information and Event Management (SIEM)
Boundary (SaaS)
Splunk
Network Exploration
Angry IP Scanner
Network Mapper (nmap)
Host Intrusion Detection System (HIDS): An IDS, via host event analysis
AIDE
OSSEC
OSSEC Enhancements/GUIs
Analytical Log Interface (AnaLogi)
Host System Monitor
Hardware
Software
Android
Linux
atop
top
iftop
ntop
Windows
AnVir Task Manager Free
Resource Monitor (resmon)
SIEM continued
ELM Event Log Monitor
EventWatchNT
Services Exploration
Nikto2
Microsoft SQL fingerprinting tool (SQL Server version determination)
Nikto2 (web server scanner)
Squid (web caching proxy)

Figure 5. Prototype Orchestration Framework recommends accelerant tools based upon the decision cycles available.

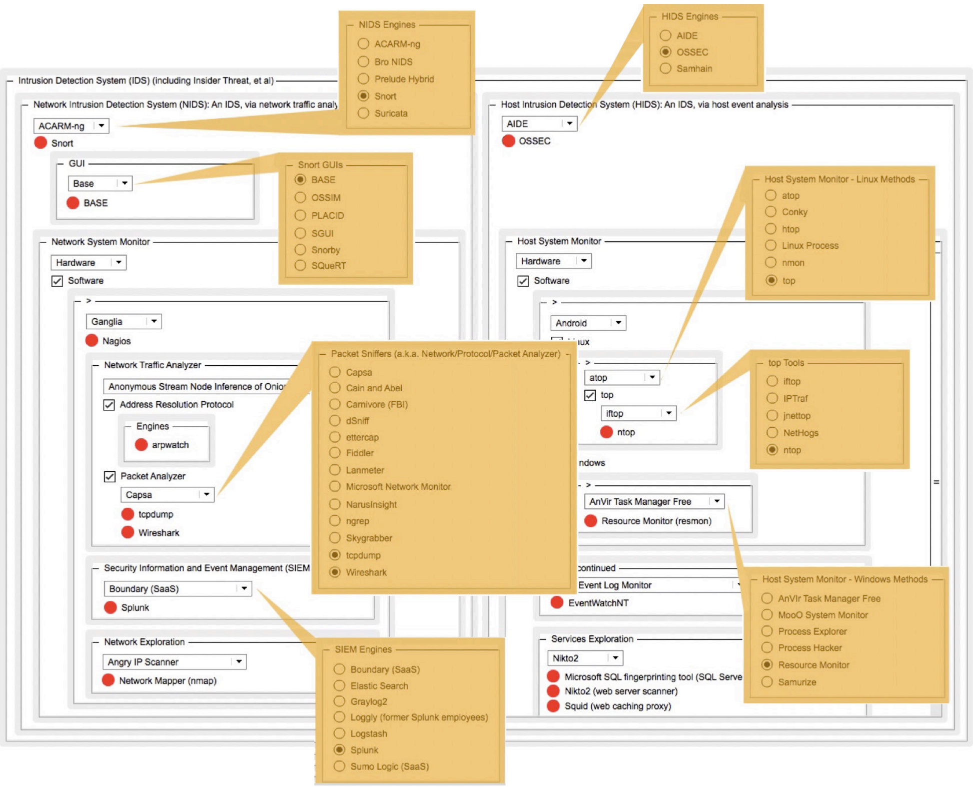


Figure 6. Prototype Orchestration Framework recommends further tools based upon the effectiveness of the prior tools utilized.

V. POSITED COGNITIVE COMPUTING PRECEPT: A TOLERANCE FOR HIGHER UNCERTAINTY

Cognitive computing aims to solve problems with naturalistic processes (e.g., human thinking). For example, a naturalistic process would segue into a decision (and manifestation) of "fight" or "flight." With funding from the Defense Advanced Research Projects Agency (DARPA), Dharmendra Modha of IBM's Almaden Research Center reverse engineered a monkey (type: macaque) brain so as to engineer one of their own, via a project called Systems of Neuromorphic Adaptive Plastic Scalable Electronics (SyNAPSE). "In May 2009, the team managed to simulate a system with 1 billion neurons, roughly the brain of a lower mammal," but the key exception was that the brain only operated at one-thousandth of real time, not enough to perform what Modha referred to as the essentials: food, fight, flight, and mating [7]. In this section, a similar case study — that of the Tyot Alba — is presented, and a supposition is put forth (as a cognitive computing precept), as to how best contend with the problem faced by Modha.

A. Precision and Accuracy

In 2009, a strain of the human influenza virus combined by random chance with a strain of swine influenza in rural Mexico, and the swine flu epidemic (involving the H1N1 influenza virus) was born. After the epidemic breached the U.S.-Mexico border, two teams of scientists offered predictions of how broadly the virus would spread throughout the U.S. Although the teams had worked independently, they produced strikingly similar results, and policy makers and scientists alike took that similarity as a sign that their predictions were accurate. Even more convincing to many were the methods by which they produced those predictions. Both groups processed prodigious amounts of data on human mobility (e.g., understanding human mobility patterns, via mobile phone records) and face-to-face interactions so as to produce a time-varying model of the nation's face-to-face social network.

To produce their predictions, both groups simulated the infection dynamics on that social network using the widely accepted Susceptible-Infected-Recovering (S-I-R) model of viral transmission. This model consisted of a set of coupled differential equations (a mathematical equation for an unknown function of one or several variables) with a small number of free parameters, and the simulation teams obtained estimates of those parameters from the Centers for Disease Control and Prevention (CDC), which seemed to be, from a *provenance* perspective, the best possible source of epidemiological statistics. Based upon all these efforts, both teams confidently concluded that about 1,000 people across the country would become infected with swine flu in the following month. Yet, by the end of that month, the number of infections was well over 100,000. The question then arose as to how the teams' estimates were askew by an error margin of 10,000%.

It turned out that the estimates of the disease's virulence, which the researchers had obtained from the CDC, were far too low. Even though the estimates had excellent *provenance*, they had poor *pedigree*; the estimates were based on reports coming out of rural Mexico, where, it turned out, many people infected with swine flu had not sought medical treatment at the facilities monitored by the public health agencies, who had then produced the estimates.

Despite the tremendous sophistication of both teams' contextual models, the models were highly sensitive to the underlying parameters. Since both teams had used the same CDC numbers for their simulations, they had produced nearly identical answers. Hence, while the estimates had excellent *precision*, they had poor *accuracy*; the teams' models consistently produced the same results, thereby demonstrating reproducibility or repeatability, but the results were far afield from the actual values.

B. Quantitative and Qualitative Data

Since the 19th century, scientists have known that the brain consists of many interacting neurons, and they have suspected that brains (hence, people) behave in the way they actually do because of the specific properties pertaining to the neuronal cells and their concomitant networked interactions. As the 20th century progressed, neuroscientists studied these properties in greater detail. They learned that electrical currents flow through neurons and across their enclosing membranes, and they studied which molecules control those currents as well as even the precise chemical processes that allow these molecules to do so. They also learned that neurons interacted at small, specific locations—synapses—at which the enclosing membranes of the neuron nearly touched. These synapses were asymmetric; one "upstream" neuron would release one of a small set of "neurotransmitter" molecules from its side of the synapse, and these molecules bound to proteins on the other neuronal cell's side of the synapse, which, in response to this binding, allowed electric current to flow into the cell. When enough electric current flowed into the cell within a relatively short period of time (**about 1 millisecond**), it triggered the downstream cell to release neurotransmitter molecules from a different set of synapses for which *it* was the upstream cell. In terms of overall architecture, all the neurons in the brain are linked by an intricate Web of these synapses, which is sufficiently complex to produce the complex set of behaviors that include memory recall on how to perform a specific action.

However, for the neuroscientist, it was difficult to measure the strength of the interaction between two cells grown in a lab, and it was even harder to measure the connection strengths within an intact brain. Subsequently, scientists adopted a simple model of this complex biophysical system, which they termed a *neural network*. This simplified model included a set of neurons, a listing of which particular neurons had made synapses onto each other, as well as a listing of the strength and sign of those synapses (whether they caused current to flow in or out of the downstream cell). Various *neural network models* used more or less complex models to describe the biophysics within neurons: (1) some used a discrete-time process, for which, at each time-point, all the neurons would simultaneously update the signals they sent out of their upstream synapses, based upon the signals they received at the previous time point; (2) more complex approaches used differential equations to model the interactions of incoming signals from different times and non-linear response functions (such as the work of Stanford University School of Medicine's Harley H. McAdams) to calculate the neuron's output from its time-weighted input.

Unfortunately, neuroscientists did not have access to all the requisite information needed to construct even minimalistic models for a real brain (the human brain has ~100 billion neurons and ~100 trillion synapses). However, through careful behavioral experiments, paired with measurements of some of the connections within certain parts of the brain, and the electrical currents flowing through those neurons, scientists have been able to apply the *neural network model* to offer possible explanations for many brain functions.

To provide some insight into the complexity, Knudsen and Konishi's 1978 work on the Tyot Alba (a.k.a. "barn owl" or "common barn owl") is introduced; a series of careful behavioral experiments in the 1980s revealed that barn owls have the ability to very precisely locate the source of a sound, via interaural time difference and interaural level difference. In essence, the barn owl achieves the requisite and apropos "right-left" sound localization (ability to identify the location or origin of a detected sound in direction and distance [8]) by calculating the time difference between sounds arriving at its two ears. A very quick calculation reveals that the time difference will be less than **.1 milliseconds**, meaning that for the barn owl to utilize the changes within that difference to calculate position, it must be sensitive to differences an order of magnitude smaller or even beyond (e.g., approximately **.01 milliseconds)**. However, as described previously, neurons in the neural network model respond to inputs averaged at roughly **1 millisecond and beyond**, meaning that the *neural network model* does not adequately explain the barn owl's aural system.

The explanation turns out to involve the interplay of the spatial organization of the connections between the neurons within the system coupled with subtle biophysical differences between the effect of signals that arrive through adjacent synapses as well as the signals that arrive at distant synapses. Hence, to understand how barn owls locate sounds, it is necessary to know not only which neurons are connected to each other, but also their specific biophysical properties, the exact spatial locations in which they connect, and the detailed shapes of the neurons within the network as well as the overall shape of the [neuronal] network. In other words, it is essential to have a comprehensive knowledge of the *morphology, epistemology,* and *praxis* of the system [9];

attempts to simplify the description too much results in a loss of ability to explain the effect being studied.

In modern times, it has been noted that many elegant quantitative models do not well describe natural phenomena, and the notion of quantitative (in)exactitude has challenged the promise of exponential increases in computing power. After all, data comes in two forms: *quantitative data* (data that can be measured) and *qualitative data* (data that can be observed, but not necessarily definitively measured — e.g., textures, smells, tastes). However, for both cases, the processed data still constitutes information.

C. Uncertainty and Ambiguity

Oftentimes, the desire to lower *uncertainty* (a lack of information) and achieve quantitative definiteness "overshadows" the need to lower *ambiguity* (a lack of clarity or context around the information). While reducing *uncertainty* is linear, reducing *ambiguity* is iterative. By way of example, an answer in response to a question temporarily reduces *ambiguity*. However, in answering the question, it leads to more questions, with more questions begetting more answers, and so on. Each answer is responsive to that specific question, but by being successive (and iterative), it only slightly reduces the *ambiguity* around the initial query.

Within these environs of ambiguity, decision-making typically occurs before the full context and consequences are known, as much of learning is derived from retrospection, and any delays may render the information-at-hand out-of-date. Hence, for decision-making amidst compressed decision cycles, it is preferable to have lower *ambiguity* and higher *uncertainty* so as to more closely approximate real-time responsiveness. Given this *uncertainty-ambiguity* paradigm, if an orchestration framework can successfully leverage reduced *ambiguity* for an isomorphic problem (i.e., similar to a previous problem, which has been solved) from another situation, higher *uncertainty* will be tolerated assuming the lower *ambiguity*. Hence, the criticality of a repertoire of veteran methodologies and tools (at machine-speed) to achieve this lower *ambiguity* should be axiomatic. Indeed, if this is accomplished (the ability of computer systems to stimulate and complement human cognitive abilities of decision-making), a subtle advance in cognitive computing will have been made.

VI. POSITED ARTIFICIAL INTELLIGENCE PRECEPT: DESIRE FOR GESTALTIAN CLOSURE

The Turing Archive for the History of Computing defines AI as "the science of making computers do things that require intelligence when done by humans" [10]. Practitioners often explain the relationship among AI, Machine Learning (ML), and Deep Learning (DL) as follows: AI is the idea that came first, ML blossomed afterwards, DL is driving AI's explosion, and Deep Belief is currently of keen interest.

A. Deeper Belief amidst Compressed Decision Cycles

In accordance with the Shannon-Weaver sender/receiver model of communication, a receiver makes a zeroth-order approximation of the sender's intended connotational meaning, wherein connotational meaning is determined from semantic context (e.g., historical, cultural, political, institutional, social, et al), such as the sender's social behavior (e.g., inflection, facial expressions, body language, proxemics, et al). Then, utilizing what Richard Palmer termed the "constant process of interpretation" [11], the receiver recursively makes higher-orders of approximation as more semantic contextual information becomes available. For all practical purposes, there are finite successive interpretants because, according to linguist Louis Hjelmslev, the interpretation of the sender's intended meaning is constitutive of, and thereby limited to, the receiver's life experiences. Consequently, according to the founder of analytical psychology, psychiatrist Carl Jung, while the symbol may be apprehended by the receiver at the conscious level, the archetypes, which inform it, exist only at the unconscious level; these archetypes are representative of unlearned tendencies, similar to the concept of instincts discussed by the founder of psychoanalysis, neurologist Sigmund Freud, to experience things in an individualized fashion, and in most cases, the receiver's desire for "Gestaltian Closure" leads to an assignment of a low-order approximation based upon these inherent biases or archetypes. Given compressed (i.e. reduced) decision cycles, a special variant Deep Belief Network (DBN) may be leveraged as a "Gestaltian Closure" accelerant to expedite matters.

B. DBN over DL for Gestaltian Closure admist Compressed Decision Cycles

- *Artificial Intelligence (AI).* According to Steve Hoffenberg of VDC Research, "In an artificial intelligence system, the system would have told … [us] … which course of action to take based on its analysis. In cognitive computing, the system provides information to help … [us] … decide" [12];
- *Machine Learning (ML).* Some AIs utilize ML. This subset of AI is predicated upon algorithms that can learn from and make predictions based upon data; instead of following a specific set of rules or instructions, these algorithms are trained to detect patterns within large amounts of data;
- *Deep Learning (DL).* In general, DL furthers ML by taking the processed information output from one layer and feeding it as input for the next layer;
- *Deep Belief Network (DBN).* Generally speaking, DBNs are Generative Neural Networks (GNN) that stack Restricted Boltzmann Machines (RBMs). While DBS can become complex, in many cases, they still outperform many existing methods of prediction.

C. Higher Tolerance for Uncertainty amidst Compressed Decision Cycles

As discussed previously in Section V, higher *uncertainty* will be tolerated assuming lower *ambiguity*. This cognitive computing precept may be leveraged as an accelerant to expedite matters amidst compressed decision cycles. When combined with a special variant DBN, which may also be leveraged as an accelerant, a unique pathway for decision-making is presented, as shown in Figure 7. By way of explanation, data is ingested by two disparate pathways: (1) Uncompressed Decision Cycles (UDC), and (2) Compressed Decision Cycles (CDC). For UDC, the data is passed for Deep Learning (DL) as well as a paradigm of "Higher Ambiguity and Lower Uncertainty" (HALU) (i.e. more data is desired). In contrast, for CDC (the entire pathway is shown in red within Figure 7), data will be passed to a Deep Belief Network (DBN) and a "Lower Ambiguity and Higher Uncertainty" (LAHU) module. For the UDC pathway, DL and HALU pass their votes to a modified N-Input Voting Algorithm (NIVA) 1 module [13], whose output is then passed along to a modified Voting Algorithm for Fault Tolerant Systems (VAFTs) module for further processing [14] prior to a decision being reached. For the CDC pathway, DBN and LAHU pass their votes down a fast track pathway that has its own modified NIVA 2 module, an additional "Lower Ambiguity Accelerant (LAA)," and a resultant decision. It should be noted that the NIVA modules (NIVA 1, NIVA 2) are custom coded variants. The VAFTS module is also a custom coded variant. It should further be noted that the multi-threaded custom coding (as contrasted to single-threaded) and the inclusion of glue code constituted a non-trivial endeavor.

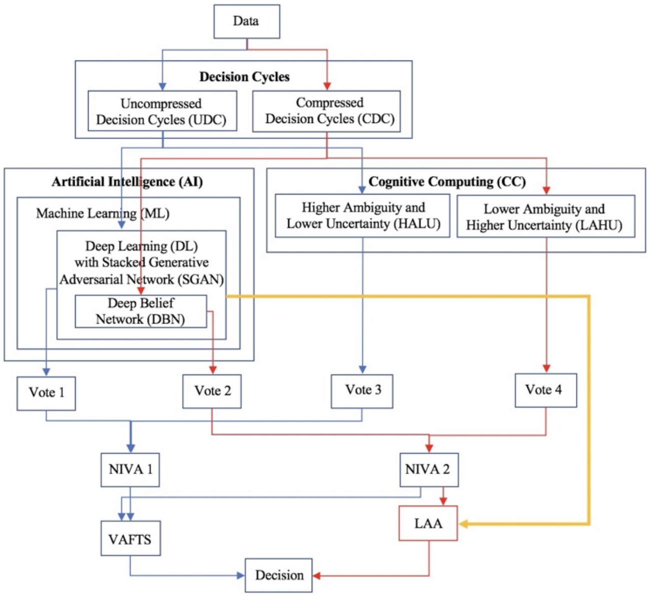

Data
Decision Cycles
Uncompressed Decision Cycles (UDC)
Compressed Decision Cycles (CDC)
Artificial Intelligence (AI)
Machine Learning (ML)
Deep Learning (DL) with Stacked Generative Adversarial Network (SGAN)
Deep Belief Network (DBN)
Cognitive Computing (CC)
Higher Ambiguity and Lower Uncertainty (HALU)
Lower Ambiguity and Higher Uncertainty (LAHU)
Vote 1
Vote 2
Vote 3
Vote 4
NIVA 1
NIVA 2
VAFTS
LAA
Decision

Figure 7. Hybridization of a "Lower Ambiguity and Higher Uncertainty" precept with a "Deeper Belief amidst Compressed Decision Cycles" precept.

Overall, the cognitive computing precept accelerant, when hybridized with a special variant DBN accelerant, yielded a unique pathway for decision-making.

VII. Experimental Results from the Hybridized Computational Methodology

The goal of the experimental testing was to ascertain how the prototype orchestration framework performed when benchmarked against acknowledged performance metrics. Two separate cyber testbeds on a single cyber range, as well as a designated cyber platform for education, training, evaluation and exercise (ETEE) were utilized for the experiment. The results from the two testbeds were averaged for the purposes of Figures 8 and 9 below. Stable operations for the prototype orchestration framework equated to less than 6 days. Results for the Months/Years category were not applicable, as the various iterations were all less than a week (i.e. 1-5 days); likewise, results for the Weeks category were not applicable. Nevertheless, when benchmarked against some percentages from the well-known Verizon Data Breach Investigations Report (whose results have been combined in some cases — e.g., months with years — for the purposes of benchmarking), sub-week results were promising. The time from "initial compromise to discovery" shifted to minutes rather than hours or days. The time from "discovery to containment or restoration" shifted to minutes rather than days. The time from "initial attack to initial compromise" was pushed out to days rather than minutes, and the time from "initial compromise to data exfiltration" was pushed out to days rather than minutes or hours. Further investigation is needed with regards to the slight degradation in performance after several days (i.e. 6+ days) against the programmed advanced persistent threats (APTs) of the involved testbeds.

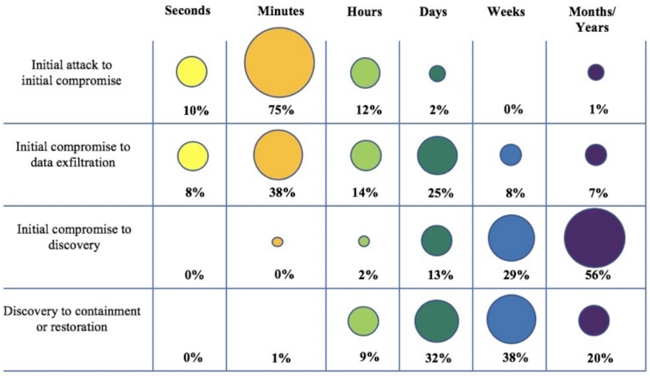


Figure 8. Verizon Data Breach Investigations Report (VDBIR) (whose results have been combined in some cases — e.g., months and years — for the purposes of benchmarking).

ISBN: 978-1-61208-683-5

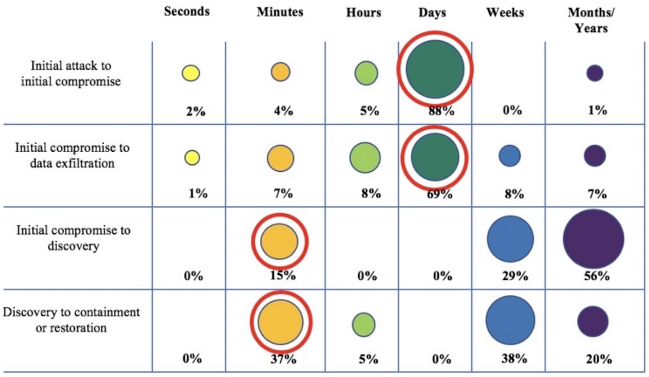


Figure 9. Performance Results of the Prototype Orchestration Framework Benchmarked against the Results of the Verizon Data Breach Investigations Report.

Overall, the experimental testing demonstrated that the prototype orchestration framework, which incorporated, among other notions, an artificial intelligence precept with a cognitive computing precept (i.e., hybridization of the LAHU precept with a DBN precept), proved promising (as demonstrated by the aforementioned results) when benchmarked against the acknowledged performance metrics.

VIII. Posited Key DL Paradigm and LAA Feeder

A. DL with SGANS Paradigm

The contributory DL vote stems from modified [Deep Convolutional] Generative Adversarial Networks (GANs) [15], each of which is comprised of two *neural networks,* which are pitted against each other (hence, the "adversarial" aspect in an unsupervised machine learning paradigm). The generative aspect is best described by contrasting it to a discriminative aspect. Whereas discriminative models endeavor to learn the boundary between classes (given the labels y and features x, the formulation p(y|x) equates to "the probability of y given x"), generative models endeavor to model the distribution of individual classes (the focus is on "how you get x," and the formulation p(x|y) equates to "probability of x given y" or the probability of features given a class). GANs are well known for being able to, for example, find the roads on an aerial map, fill in the missing details of an image (up sampling, given the edges), and construct an image, which postulates how a person might look when they are older [16]. For this experiment, the GANS are stacked; hence the paradigm is that of Stacked Generative Adversarial Network (SGAN).

B. LAA, via DL Feeder

As previously discussed, the higher need for cognitive closure [17] drives a tolerance for higher *uncertainty* given a state of relatively lower *ambiguity* (a repertoire of examples of successively handling similar problems). A key factor for achieving this steady state of relatively lower *ambiguity* resides in the ongoing learnings of the SGAN in the DL module. This feeder mechanism, which is comprised of the SGAN in the DL as well as the LAA, was previously shown in orange within Figure 7.

IX. Conclusion

This paper presents the benchmarked performance results of a prototype orchestration framework. The premise for devising such a system was predicated on the ever-increasing cycles of adaptation of cyber-attackers leveraging an array of potential accelerants (e.g., NVD, SHODAN, etc.). The presented system utilizes several accelerants in an attempt to mitigate, via a cyber defense accelerant for particular high exposure dimensions (e.g., network, software attack surfaces). For the UDC pathway, DL and HALU passed their votes along to a modified NIVA 1 module and VAFTS variant. For the CDC pathway, DBN and LAHU pass their votes down a fast track pathway; this pathway is facilitated by a LAA, which has been continuously informed by the SGAN from the DL module. The described work has been benchmarked, via an ETEE, against various permutations generated by the testbeds of the involved cyber range and compared to the presented VDBIR. The preliminary results of the modified SGAN-DBN-NIVA-VAFTS amalgam seem promising. Future work necessitates a further investigation of any degradation in performance, as well as the potential involvement of other useful algorithmic modifications. Collaboration MSSPs have concurred that the discussed modified DBN (within the AI->ML->DL paradigm) and LAHU as well as their modified SGAN-fed LAA, particularly amidst CDC, warrant further research.

Acknowledgment

The author would like to thank the Decision Engineering Analysis Laboratory (DEAL) for its encouragement and motivation throughout the process of pursuing and completing this research. Without their initial and continuing assistance, as well as the ideas, feedback, suggestions, guidance, resources, and contacts made available through that support, much of this research would have been delayed. The author would also like to thank VT & IE^{2}SPOMTF. This is part of a paper series on enhanced event correlation. The author would like to also thank USG leadership (e.g., the CAG). In addition, the author would like to thank ICE Cyber Security for the opportunity to serve as Chair, Scientific Advisory Board. The author would further like to thank the International Academy, Research, and Industry Association (IARIA) for the constant motivation to excel as well as the opportunity to serve as a contributing IARIA Fellow within the cyber and data analytics domains, particularly in the area of mission-critical systems.

References

[1] "What You Need to Know About Managed Services," CISCO Public, p. 3, 2017.

[2] "Managed Services Market Worth $193.34 Billion by 2019," PR Newswire, pp. 1-4, 7 January 2015.

[3] "FM 3-38 Cyber Electromagnetic Activities," Department of the Army, pp. 1-2, 12 February 2014.

[4] E. Tabor, "3 Ways Managed Services Provide Access to the Most Advanced IT Tools," ISG Technology, pp. 1-2, 11 January 2017.

[5] D. Dinely, "The Greatest Open Source Software of All Time: InfoWorld's Open Source Hall of Fame Recognizes the 36 Most Important Free Open Source Software Projects in History (and Today)," InfoWorld, pp. 1-2, 17 August 2009.

[6] J. Porup, "What is Wireshark? What This Essential Troubleshooting Tool Does and How to Use It," CSO, IDG Research, pp. 1-8, 17 September 2018.

[7] R. Kay, "Cognitive Computing: When Computers Become Brains," Forbes, pp. 1-5, 9 December 2011.

[8] B. Nelson and T. Takahashi, "Independence of Echo-Threshold and Echo-Delay in the Barn Owl," PLOS One, pp. 1-11, 31 October 2008.

[9] G. Ritter, "An Introduction to Morphological Neural Networks," Pattern Recognition, Proceedings of the 13th International Conference on Pattern Recognition, vol. 4, pp. 709-717, 1996.

[10] D. Evans, "Cognitive Computing Vs. Artificial Intelligence: What's the Difference?" Tech Innovation, pp. 1-11, 28 March 2017.

[11] R. Palmer, Hermeneutics: Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer. Northwestern University Press, 1969, p. 283.

[12] S. Hoffenberg, "IBM's Watson Answers the Question, 'What's the Difference Between Artificial Intelligence and Cognitive Computing'," IDC Research, pp. 1-3, 24 May 2016.

[13] A. Karimi, F. Zarafshan, and A. Ramli, "A Novel N-Input Voting Algorithm for X-by-Wire Fault-Tolerant System," The Scientific World Journal, pp. 1-9, 2014.

[14] S. Latif-Shabgahi, "An Integrated Voting Algorithm for Fault Tolerant System," 2011 International Conference on Software and Computer Applications, International Proceedings of Computer Science and Information Technology (IPCSIT), vol. 9, pp. 1-17, 2011.

[15] A. Radford, L. Metz, and S. Chintala, "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks," ArXiv, pp. 1-16, 7 January 2016.

[16] C. Liu, X. Wu, and X. Shu, "Learning-Based Dequantization for Image Restoration Against Extremely Poor Illumination," ArXiv, pp. 1-10, 20 March 2018.

[17] P. Iannello, A. Mottini, S. Tirelli, S. Riva, and A. Antonietti, "Ambiguity and Uncertainty Tolerance, Need for Cognition, and Their Association with Stress," Medical Educadtion Online, vol 22(1), pp. 1-17, 2017.