COGNITIVE MACHINE INDIVIDUALISM IN A SYMBIOTIC CYBERSECURITY POLICY FRAMEWORK FOR THE PRESERVATION OF INTERNET OF THINGS INTEGRITY: A QUANTITATIVE STUDY

by

Gary C. Wong

Liberty University

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Liberty University

2023

COGNITIVE MACHINE INDIVIDUALISM IN A SYMBIOTIC CYBERSECURITY POLICY FRAMEWORK FOR THE PRESERVATION OF INTERNET OF THINGS INTEGRITY: A QUANTITATIVE STUDY

by Gary C. Wong

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Liberty University, Lynchburg, VA

2023

APPROVED BY:

Kenneth J. Hutchinson, PhD, Committee Chair

Scott D. Stenzel, PhD, Committee Member

ABSTRACT

This quantitative study examined the complex nature of modern cyber threats to propose the establishment of cyber as an interdisciplinary field of public policy initiated through the creation of a symbiotic cybersecurity policy framework. For the public good (and maintaining ideological balance), there must be recognition that public policies are at a transition point where the digital public square is a tangible reality that is more than a collection of technological widgets. The academic contribution of this research project is the fusion of humanistic principles with Internet of Things (IoT) technologies that alters our perception of the machine from an instrument of human engineering into a thinking peer to elevate cyber from technical esoterism into an interdisciplinary field of public policy. The contribution to the US national cybersecurity policy body of knowledge is a unified policy framework (manifested in the symbiotic cybersecurity policy triad) that could transform cybersecurity policies from network-based to entity-based. A correlation archival data design was used with the frequency of malicious software attacks as the dependent variable and diversity of intrusion techniques as the independent variable for RQ1. For RQ2, the frequency of detection events was the dependent variable and diversity of intrusion techniques was the independent variable. Self-determination Theory is the theoretical framework as the cognitive machine can recognize, self-endorse, and maintain its own identity based on a sense of self-motivation that is progressively shaped by the machine's ability to learn. The transformation of cyber policies from technical esoterism into an interdisciplinary field of public policy starts with the recognition that the cognitive machine is an independent consumer of, advisor into, and influenced by public policy theories, philosophical constructs, and societal initiatives.

Keywords: Cyber public policy, cognitive machines, symbiotic cybersecurity, social IoT

Dedication

1 Corinthians 13:4-6 states, “Love is patient, love is kind. It does not envy, it does not boast, it is not proud. It does not dishonor others, it is not self-seeking, it is not easily angered, it keeps no record of wrongs. Love does not delight in evil but rejoices with the truth. It always protects, always trusts, always hopes, always perseveres”. This dissertation is dedicated to my wife Cathy and my son Greyson for their love, support, and patience throughout this doctoral journey. I would not have gotten here without them. You mean the world to me, and I love both of you with all my heart.

Acknowledgments

I must acknowledge God for His guidance, inspiration, wisdom, and strength throughout this journey. I want to thank everyone who inspired me to learn, challenge myself, and do what is right on the path to becoming the person I am. I would like to thank my Chairperson, Dr. Kenneth Hutchinson, and my Reader, Dr. Scott Stenzel, for their assistance and encouragement every step of the way throughout this process as I could not have had a better support system on this academic journey. I would also like to extend personal gratitude to my mother, Mrs. Pauline Wong, who showed me what true determination and wisdom is and my late father, Mr. Ming Wong whose personal sacrifice is what kept our family afloat in the years after we immigrated. I would like to thank my brother Mr. Terry Wong and his wife Mrs. Azenith Gueco for their positive encouragement and their reminder that life is more than just what is in front of you. I would like to thank my in-laws (Mr. and Mrs. Paul and Dorothy Kotsenas), my sisters-in-law (Dr. Amy Kotsenas (and her husband Dr. Ron Kuzo) and Ms. Beth Kotsenas), and my aunt-in-law Mrs. Joanne Cavazos for each had a part in encouraging me to keep going. With gracious love and humor, I would like to thank our fur-babies; I started this journey with Sunshine and Mojo, our beagle mix and basset hound respectively. Sadly, both crossed the Rainbow Bridge before I got to this point. Bearing witness to the journey's completion are Ryleigh and Pickles, our shepherd mix and chihuahua mix; dogs really are angels on earth. Additional gratitude is extended to Mr. and Mrs. Steven and Samantha Willits, Dr. Elizabeth Kraft-Weiss, Dr. Peter Babich, colleagues Dr. Frances Deutch, Mr. Victor Matamala, Mr. Michael Esparza, and Mrs. Stephanie Ludovici (the latter three aspiring to or having started their own doctoral journeys), Mr. Sheldon McCabe, Mr. Jacob Coons, Mr. Chris Giamo, and Mr. Philip Doll. Last, but certainly not least, I would like to thank my brothers and sisters in the US Armed Forces for their continued sacrifice and vigilance in the defense of our great Nation.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

APT	Advanced Persistent Threats
CCP	Chinese Communist Party
CET	Cognitive Evaluation Theory
DCS	Data-centric Security
DID	Decentralized Identifier
DPKI	Decentralized Public Key Infrastructure
DNS	Domain Name Server
DLL	Dynamic Link Library
H2H	Human-to-Human
H2M	Human-to-Machine
HMT	Human-Machine Teaming
IoT	Internet of Things
M2M	Machine-to-Machine
PRC	People's Republic of China
PKI	Public Key Infrastructure
SDT	Self-determination Theory
SSI	Self-sovereign Identity
TA	Trusted Agent
URI	Universal Resource Identifier
VC	Verifiable Credential

CHAPTER ONE: INTRODUCTION

Overview

The Internet of Things (IoT) is an interrelated technological and social systemic environment enabled through data transference (Smith et al, 2021). The IoT links technological innovation, user behavior, and business processes to create digital ecosystems that "integrate communicating "things" and human users as a single entity" (Sheron et al 2019, p. 1). Securing the IoT is not simply a matter of deploying network perimeter defense tools as modern adaptative threats transform data into a weapon to alter attack vectors and intrusion techniques dynamically. Machine cognition and the social IoT replicates societal concepts which have significant influence on physical and digital world dynamics. This quantitative study examined the complex nature of modern cyber threats to propose the establishment of cyber as an interdisciplinary field of public policy initiated through the creation of a symbiotic cybersecurity policy framework. Identity-based cognitive machine symbiotic cybersecurity policies are an interdisciplinary approach to codifying machine manifestations of autonomous behavior, self-determination, and behavioral rationality as the cognitive machine is a symbiotic actor in the modern IoT social network. These expressions of social cognition separate the cognitive machine from traditional artificial intelligence as they are "designed to either detect and respond to social signal in the environment" (Cross and Ramsey 2021, p. 201) in a manner that humans perceive as social interaction (Cross, 2021). Furthermore, cognitive machines are "capable of clustering, classifying, and making sense of the unstructured data that describe the world in which we live" (Schuetz et al 2020, p. 463) establishing a bilateral relationship between humans and machine partners. The interdisciplinary approach explores the socio-technical foundation of digital identities for humans and cognitive machines within the social paradigm of the IoT.

Creating shared understanding of socio-technical digital identities could determine critical attributes comprising individual digital uniqueness. Codifying what those attributes are could inform the establishment of mechanisms for behavioral self-verification and identify business processes for maintaining attribute legitimacy to preserve IoT integrity. Properly constructed policies enable granular controls over resource (data, services, and applications) access and user credential management as vulnerabilities in trust are the focal point for malicious intrusions and exploitations. The purpose of this study is to postulate a design framework for symbiotic cybersecurity policies incorporating cognitive machine individualism to enhance the implementation of human-machine teaming (HMT) in the preservation of IoT integrity. As the cognitive machine is a symbiotic actor in cyberspace, legitimate communication (and interaction) requires the ability to distinguish discreet entities as our digital identities are nothing more than transactional data. If our policies recognize that there is a social relationship between humans and cognitive machines (and between machines) in the IoT, then there is potential for the creation of a common entity-based cyber policy framework for constructing, maintaining, and verifying the digital identities of both humans and machines in cyberspace that fuses behavioral and social principles of trust with technological innovation. This common policy framework could create standards of governance for establishing and maintaining cyberspace digital legitimacy. This proposed framework complements the collaborative (and communicative) aspects of human-machine teaming (HMT) to mitigate the shortfall "that the internet was created without an identity Layer" (Davie et al 2019, p. 46). Facilitating trust between cognitive team members in the IoT "requires scalable and trustworthy digital identification management services" (Samir et al 2022, p. 7972) for internet technologies and their associated applications, services, and devices. The academic contribution of this research project is the fusion of

humanistic principles with IoT technologies that alters our perception of the machine from an instrument of human engineering into a thinking peer to elevate cyber from technical esoterism into an interdisciplinary field of public policy. This impacts and disrupts future research paradigms (particularly in the public policy, behavioral sciences, social sciences, and cyber domain) as the IoT and adaptive modern technologies has enabled a potentially emergent concept of a machine society that is equal to (but independent of) human society. The contribution to the US national cybersecurity policy body of knowledge is a unified policy framework (manifested in the human-cognitive machine symbiotic cybersecurity policy triad comprised of digital identity legitimization, digital identity legitimization, trust and positive reputation, and ethical motivation) that could transform cybersecurity policies from network-based to entity-based.

Background

The IoT's automated, increasingly autonomous, and symbiotic, nature underpins the critical role of digital identities for preserving systemic integrity and resiliency as cognitive machines function as independent data producers and consumers. The core of the IoT is data transference through human-to-human (H2H), human-to-machine (H2M), and machine-to-machine (M2M) interactions. Data's persistence enables many attack surfaces as digital elasticity accelerates the adversarial threat cycle due to "sophisticated technologies once accessible exclusively to a few global powers are increasingly available and affordable" (Srivastava 2019, p. 58). The IoT is composed of "billions of intelligent communicating 'things'…cater diverse services to Information Technology (IT) users" (Jurcut 2020, p. 192) using a scalable, distributed, and heterogeneous architecture of attributable protocols and applications. This architecture is "an enabler of automated and convenient lifestyles for modern-

day humans" (Adi 2020, p. 16205). Implementation of identity-based symbiotic cybersecurity policies aligns the dynamic nature of human behavior (Steadman and Scott-Hayward, 2021) with data itself as its transferal enables the prediction (or control) of the future state (Chatfield and Reddick, 2019) through "sensor/actuators, communications/connectivity, data analytics and security, and smart applications" (Chatfield 2019, p. 349). Modern malicious cyber threats prioritize data exploitation, cyber extortion, and social media disinformation to achieve their objectives; their activities account for "40% of all threats to computer networks globally costing entities between US$40 billion to US$1 trillion annually" (Al-Matareh 2020, p. 19). Identity-based cognitive machine symbiotic cybersecurity policies require the establishment of digital uniqueness whose attributes safeguard "physical and digital assets against illegal access, copying, modification, disclosure, destruction, and transfer to third parties for personal gain" (Mishra et al 2022, p. 9). The development of these policies integrates data security with dynamic access and identity credentials management extending beyond the traditional network or perimeter-based bastion paradigm. The difference between the IoT and previous industrial systems is the "connectivity of things to the Internet and their wider scope of application" (Chatfield 2019, p. 350). The current body of literature provides valuable insight into the interdependent nature of data and digital identities (Kang, 2020; Sedlmeir, 2020; Susanto, 2018) for formulating a multi-disciplinary approach to threat mitigation (Rasouli, 2020).

Introduction to Self-determination Theory

Self-determination Theory (SDT) is the theoretical framework of the study as cognitive machines are "systems with the ability to adapt to changes in its environment and be able to learn from experience" (Skilton and Hovsepian 2017, p. 121). The experiential facet is an important component as the "individual development of our character is not only dependent on our

environment…but also on our decisions" (Nida-Rumelin and Weidenfeld 2022, p. 22). Decisions made through experience influence the creation of virtues as future beliefs and attitudes are changed (Nida-Rumelin, 2022). The ability to modify environments and transmit those modifications through language separates humans from other creatures in the natural world (Saetra, 2019). Through sophisticated modern machine learning (or ML) algorithms and environmental sensing, cognitive machine can acquire measures of autonomous decision-making and expressions of behavioral rationality (Saetra, 2019) mimicking (or replicating) humanistic adaption. SDT focuses on the "inherent motivational propensities for learning and growing, and how they can be supported" (Oppl and Stary 2022, p. 8). Through this theoretical focal point, the postulation is that the cognitive machine can recognize, self-endorse, and maintain its own identity based on a sense of self-motivation that is progressively shaped by the machine's ability to learn. Identity governs the "operations, ownership, and autonomy" (Haber and Rolls 2019, p. 28) of cognitive machines; pairing identity with social behavior mimicking the human persona requires a framework capable of exploring machine motivation that extends beyond programmed responses. As cognitive machines can advance their abilities and "establish new behavior patterns via labeled data with machine learning" (Agrawal et al 2020, p. 192), important questions must be asked regarding what constitutes machine digital distinctiveness and if underlying societal influences are shaping that distinction. Cognitive computing is a system that "learns at scale, reasons with purpose and interacts with humans naturally" (Sathi 2016, p. 6), as these intelligent agents can "learn complex tasks, interact with humans via natural interfaces and make autonomous decisions and actions working with individual and groups" (Sathi 2016, p. 6). The power of machine cognition has fundamentally altered the landscape of digital interfaces as ML enables them "to make sense and be appropriately fast enough to fix the problems or

opportunities at the speed the situation requires" (Skilton 2017, p. 213). The detection and response capabilities of cognitive machines span motion detection, active listening, and voice dialog encompassing recognition of human emotion, speech patterns, nonverbal cues, and machine verbal response (Sathi, 2016) that enables the machine to mimic, adapt to, or interact with a human partner.

Modern malware is designed for virtual espionage and sabotage (Alenezi et al, 2020) based on a trust concept where users assume that IoT interactions are between legitimate parties. The lack of cognitive machine digital identity uniqueness is a point of malicious exploitation as machines do not possess an individually determined (and managed) set of certifiable credentials differentiating them from one another. For example, two smart homes might have *Alexa* working on their essential functions. Current cybersecurity policies governing digital identity architectures do not permit one instance of *Alexa* to self-identify as "Bob" and the other as "Sally", so that "Bob" and "Sally" interact as trusted IoT entities due to their credentials. As "Bob" and "Sally" adjust to different home operating environments, their distinctions increase over time and affect their IoT identity credentials (just like changing height and weight affects human physical identity credentials). In effect, "Bob" and "Sally" become intrinsically unique due to their ability to learn and adapt; their identities are their own, with each machine possessing the proper claims to prove them. In the physical world, we are born with traits of individuality that are non-translatable in the digital world as our identities are decomposed into transactional data that mingle with other data streams in the IoT. Therefore, human digital identities are artificial constructions requiring humans to constantly endorse their authenticity and distinctiveness. Cognitive machine identities must maintain a similar structure as their individualistic characteristics influence autonomous behaviors and the effectiveness of pairing

within an HMT framework. Policies acknowledging machine digital distinctiveness are premised on the realities of cognitive pairing between humans and machines as our digital identities are co-mingled data streams within the IoT. In HMT, cognitive partners require mechanisms to construct, attribute, legitimize, self-validate, and present their identities to other parties within the IoT chain of trust.

Status of Digital Identity Research

The body of contemporary research has progressively shifted from the network-centric paradigm associated with traditional cybersecurity to the data-centric paradigm of the IoT that elevates the importance of digital identities for secured data access control and user authentication. The rise of dynamic, advanced persistent threats (APTs) utilizing complex data intrusion and exploitation methodologies has prompted researchers to delve into the principles of proactivity and deliberative cyber defense adaptions leveraging multi-nodal, multi-functional, and multi-layered mechanisms (Berrada, 2020; Quintero-Bonilla, 2020; Xie, 2020). Digital identities contribute to predictive analytics by coupling artificial intelligence (AI) with behavioral sciences to create innovative behavior-based threat countermeasures, sentient-based access control, and ML-enabled vulnerability assessments (Baski, 2021; Zulkefli, 2020; Jiang, 2020; Addae, 2019). Identity management and assurance are direct influences on the preservation of trust within the IoT as digital identities are inherently transactional with "attributes that can be revoked, deleted, transferred, or exchanged" (Sedlmeir 2020, p. 604). Effective identity management mechanisms adopt a multi-disciplinary approach spanning compliance, standards, processes, policies, credential lifecycle management, service access, data repositories, rules of behavior, analysis, and reporting (Rasouli, 2021). Furthermore, digital identities are a medium of exchange requiring a cyber defense governance structure

encompassing physical and logical objects to facilitate "efficient and fine-grained management of attributes" (Yang 2020, p. 2) associated with the components that build them.

Assumptions

The data-centric paradigms of the IoT have increased the cost of cyber defense as the adaptive heuristics of adversarial threats extend beyond network boundaries since data itself is a platform that can be weaponized or exploited. The assumptions associated with this study are below:

A1 - Malicious actors are organized entities utilizing standard and specified cyber intrusion tools to harvest data from target IoT environments.

A2 – Human-Machine Teaming is a core paradigm of IoT-related cybersecurity policies.

A1 assumes that malicious actors "apply resources in deliberate ways to attack…assets" (Ahmad 2019, p. 403) as "getting data out of a target environment is as important as getting into the environment itself" (Borges, 2021, p. 199). The fundamental aspect of the IoT is that data is sensed (or collected), processed, adjusted, represented, and integrated (Tsiatsis et al, 2018) into "diverse applications, or to perform computations on it…in order to extract business value and associate it with respective business needs" (Tsiatsis, 2018, p. 112). Malicious actors will utilize data to conduct reconnaissance operations as their objectives are "often to act on a specific target and get out" (Borges, 2021, p. 184); credential dump attacks are a common intrusion tactic that places user authentication information into the public domain and permits malicious actors to glean information that allows ingress into a targeted environment using compromised credentials to gain access. Malicious actors can dump stolen data onto the internet using compromised third-party services or place it in public to maintain their anonymity (Borges, 2021). IoT-related policies to strengthen digital identities (particularly in adapting them to cognitive machines) are

countermeasure techniques to prevent (or reduce the probability of) malicious actors from conducting reconnaissance through the theft of credentials or masquerading as legitimate users. Limiting the ability of malicious actors to use compromised identities and credentials is critical as the IoT "can involve a large set of different actors providing services and information that need to be composed and accessed with different levels of aggregation" (Tsiatsis, 2018, p. 53). As the architecture of the IoT is heterogeneous, identity-based symbiotic cybersecurity policies are a mechanism for maintaining systemic resilience as its consistent structure provides replicability of best practices so that solutions to problem sets can be reused (Tsiatsis, 2018).

A2 recognizes that the IoT blurs the line between the physical and digital worlds (Moallem, 2019) where humans can view the certificate attributes that create distinctiveness in the virtual space. Still, verification of that uniqueness cannot occur without software applications (Moallem, 2019). The connected devices of the IoT must identify themselves (Moallem, 2019) yet, cognitive machines do not possess biometric traits to convert aspects of physical identities into digital ones. For the estimated "34 billion IoT devices" (Moallem, 2019, p. 52), the constraints posed by the lack of physical attributes requires an adaptive approach combining unique identifiers with behavioral attribute replication where digital identities are self-validated. Identity-based cognitive machine symbiotic cybersecurity policies advocate for cyber defense initiatives capable of operating at scale as M2M interactions need the ability to "automatically generate machine identities" (Moallem, 2019, p. 70) to mitigate the possibilities of compromise and exploitation. Prevention of malicious software exploitations through the verification of machine identities takes on significance as cognitive IoT devices perform diverse societal functions such as monitoring hospital operating procedures, detecting weather pattern changes, connecting automobiles, and biometric identification where "data collected…may be processed

in real-time to improve the efficiency of the entire system" (Khan and Salah, 2018, p. 395). Data preservation extends beyond the H2M and M2M transactional characteristics of social media or finances as data is the foundation through which humans can team with machines for basic human functionalities. Identity-based symbiotic cybersecurity policies are a consideration that data is an asset of the IoT where the "proper implementation of authorization and authentication…ensures a secure environment for communication" (Khan 2018, p. 397).

Limitations

The study is limited to the use of unclassified, open sources of data. No attempt to access or incorporate classified data or information related to malicious threat countermeasures or mitigation strategies, AI development plans or platforms, or US Intelligence Community-related threat monitoring and mitigation techniques are associated with the research design.

Problem Statement

The IoT increases the probability of malicious cyber activities due to its persistent capabilities to retain, handle, and transfer substantial volumes of data and information that touch many data consumers, producers, and devices. The continual propagation of cognitive machines increases the necessity of formulating cybersecurity policies that establish a shared understanding of what constructs digital identities, how attributes are created, and how those attributes are legitimized. Digital identities are the virtual representations of entities interacting within the IoT (Naik and Jenkins, 2020), self-sovereign identities (SSIs) are an emergent concept where the data consumer is in control of their digital identities (Fedrecheski et al, 2020). SSI is enabled through a verifiable credential (VC) architecture containing cryptographically signed documents with claims to the holder's identity (Ishmaev, 2020).

The problem is that current US national cybersecurity policies operate on the principle of implicit trust that neither enables machines to verify their identities before a data transaction is initiated nor accounts for their behavioral intent. Current network-based cybersecurity has created a fragmented policy approach, policy design, and implementation methodologies as organizations subjectively apply cybersecurity principles based on their specific technical architecture. The US Government implemented the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 as its foundational guideline for digital identities (NIST, n.d.). SP 800-63-3 states that one of its primary limitations is that it "does not explicitly address device identity, often referred to as machine-to-machine…authentication or interconnected devices, commonly referred to as the internet of things (IoT)" (NIST 2017, p. 5). Not incorporating machines into the policy framework for digital identities means that humans must implicitly trust that the machines we are communicating (and exchanging data) with are legitimate. It is this implicit trust that cyber threats are increasingly becoming more capable of exploiting as current policies do not recognize the social relationship existing between humans and cognitive machines (and between cognitive machines). The results are policies that are highly technical but fail to account for either the behavioral or social dimensions of the IoT related to H2M and M2M interactions or the inability to translate physical characteristics of individuality into the digital world. In the physical world, humans can provide proof of identity (for example, a driver's license) as those credentials are based on the individual's unique characteristics. In the digital world, traditional public key infrastructure (or PKI) methodologies attempt to replicate the same. These conventional methodologies utilize third-party Trusted Agents (TAs) to manage the issuance of digital certificates to facilitate the verification, authentication, and preservation of human digital identities. Despite the individual user having

no control over the attributes of these digital certificates (Moreno et al, 2021), PKI offers a mechanism for human users to prove their individual distinctiveness within the digital space. As cognitive machines lack individual distinctiveness, the IoT (as a conglomeration of H2H, H2M, and M2M interactions) risks increased exposure as malicious actors conduct illicit operations through identity-based exploitations targeting machine credentials in the same manner as humans. The cognitive and social behavioral relationship present in HMT could benefit from a standard policy framework governing the construction of partner digital identities to preserve their attribution and legitimacy.

Purpose Statement

The purpose of this study is to postulate a design framework for symbiotic cybersecurity policies incorporating cognitive machine individualism to enhance the implementation of human-machine teaming (HMT) in the preservation of IoT integrity. The academic contribution of this research project is the fusion of humanistic principles with IoT technologies that alters our perception of the machine from an instrument of human engineering into a thinking peer to elevate cyber from technical esoterism into an interdisciplinary field of public policy. This impacts and disrupts future research paradigms (particularly in the public policy, behavioral sciences, social sciences, and cyber domain) as the IoT and adaptive modern technologies has enabled a potentially emergent concept of a machine society that is equal to (but independent of) human society. The contribution to the US national cybersecurity policy body of knowledge is a unified policy framework (manifested in the human-cognitive machine symbiotic cybersecurity policy triad comprised of digital identity legitimization, trust and positive reputation, and ethical motivation) that could transform cybersecurity policies from network-based to entity-based. Imparting digital identity uniqueness for cognitive machines is an innovative cybersecurity

approach intended to reinforce the integrity of the IoT digital trust architecture by extending individualistic identity verification precepts. The more expansive aspect of the problem set is to explore how cognitive machine SSI can enhance the cohesiveness of future cybersecurity policies as digital partnerships propagate through HMT concepts.

Creating identity-based cognitive machine symbiotic cybersecurity policies is critical to transforming and modernizing cybersecurity and cyber defense strategies away from the traditional bastion approach. Beyond serving as attributes of trust, digital identities are aligned with the concept of entitlements whose purpose is to execute technology policies (Haber, 2019). An entitlement "grants, resolves, enforces, revokes, reconciles, and administers…access, privileges, access rights, permissions, or rules" (Haber 2019, p. 37) and is a critical part of the governance process. Data transactions and access in the IoT are centered on privileges and rights as these activities often take place outside the domain of control of any one organization or entity (Skilton, 2017). The goals of identity-based cognitive machine symbiotic cybersecurity policies are to create a comprehensive governance structure that is adaptive across the multi-layered (and distributed) components of the IoT, establish an interdisciplinary cyber public policy paradigm accounting for human and machine agents, and form cyber defense strategies to ensure IoT data interactions are conducted between legitimate parties (organic and synthetic) that possess shared intent and values.

Research Question(s)

The principal research question (RQ1) and the supporting research question (RQ2) listed below were investigated:

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

This study employed a quantitative, correlational archival data research design. For RQ1, the frequency of malicious software attacks was the dependent variable and diversity of intrusion techniques was the independent variable. For RQ2, the frequency of detection events was the dependent variable and diversity of intrusion techniques was the independent variable.

Significance of the Study

Research and the available literature indicate an increasing appreciation for the complexity of modern security dynamics and architectural requirements. The nature of the malicious actor strains the abilities of cyber defenders to develop capabilities to prevent, mitigate, and remediate intrusions and data exploitations. The IoT enables modern societies to generate more data content than in previous eras (Cheney-Lippold, 2017). As data flows openly through the interconnected IoT networks (Cheney-Lippold, 2017), the risk is the complexity and scale of cyber defense techniques required to prevent, detect, or remediate illicit data exploitation, malicious alteration, or theft. The IoT enables malicious actors to leverage technologies in a myriad of ways to organize, plan operations, and exploit vulnerabilities as the availability of data, coupled with the heterogeneous nature of the IoT, creates opportune attack surfaces since targeted data "contains real information about the owner, his actions, and the objects surrounding him" (Mustafaev and Buchaev 2020, p. 1). Digital identities within the IoT have no unique definitions (Pal, 2018) as identities can be mapped to a single entity but "an entity can have more than one identity" (Pal 2018, p. 2), thus diluting the trustworthiness of individual digital identities as billions of devices are deployed across domains spanning home applications, metropolitan monitoring, healthcare, and the defense sector (Vaidya et al, 2020). Haber and Rolls (2019) identify the three logical pillars of cyber defense as identity, privilege,

and asset (Haber, 2019) where the failure to integrate the three as the foundational principles of cyber defense models and methodologies can result in a reduction of security effectiveness as "you need to have integrated data from all three pillars to be truly effective at dealing with modern threats" (Haber 2019, p. 3).

Additionally, the connectedness of data and digital identities become essential as the IoT enables malleability in physical identities since digitization exposes people and machines to "a multitude…of ideas and principles" (Khatchatourov 2019, p. 10) that continuously influences how identity is defined in the physical world. To counteract the modern malicious actor, cyber defense models must dynamically overcome the uncertainties associated with multi-stage attack vectors and multiple attack strategies (Xie, 2021). Identity-based cognitive machine symbiotic cybersecurity policies recognize that non-human users can establish "multiple accounts, multiple credentials, and an infinite number of entitlements in its electronic format" (Haber 2019, p. 17) for H2M and M2M interactions. These policies influence emergent cyber resiliency strategies and methodologies incorporating a multi-faceted approach for data and information confidentiality, availability, and integrity (Volchkov, 2018) as HMT creates a cognitive partnership with shared IoT responsibilities.

This approach is further complicated as ML enables cognitive machines to independently scan and analyze the massive libraries of data in the IoT to "detect patterns that are outside the scope of human perception" (Dey et al 2020, p. 9). Cognitive computing is measured in degrees of self-awareness based on the "capacity of autonomy, social capacity, and pro-activity that a computer system can have to generate knowledge about itself…and determine the actions that will be executed according to that knowledge" (Andrade and Yoo 2019, p. 3). Machine cognition has altered the landscape of H2M and M2M interfaces as complex ML algorithms

increasingly enable the machine to think like humans do as “24.7% of all developers are engaging in building robotic apps and using machine learning in their projects” (Agarwal 2020, p. 193). The IoT empowers cognitive machines but exposes them to trust and data exploitations inside and across automated functions as malicious actors increasingly deploy covert communication channels to “exploit legitimate services” (Steadman 2021, p. 1).

Data and Information Security

Standards and policies form the core of the strategic approach to secured digital environments as policies provide direction for applying technical solutions to mitigate risks. In contrast, standards establish shared understanding regarding the characteristics and attributes of those solutions. Standards and policies are often the benchmarks for establishing quantifiable assessments for security measure effectiveness based on empirical information (Kang, 2020) so that data and information security could be considered business enablers and integral parts of business processes (Susanto, 2018). Furthermore, standards and policies serve to enculturate data and information security as organizational responsibilities since malicious actors seek to exploit vulnerabilities by deploying techniques that “mimic normal business logic and rely on actions that respect social norms” (Berrada 2020, p. 401).

Behavior-based Cyber Defense

The coupling of AI and ML with behavioral science to create predictive analytics promotes using cognitive machines in behavior-based defense mechanisms to execute counter-exploitation measures (Baksi, 2021). The development of this kind of risk reduction model is predicated on the cognitive machine conceptualizing the variables of intrusion tactics and techniques and coupling them with the probability of detection so that it deploys defensive measures across the phases of an intrusion and exploitation attempt (Huang, 2020). Counter-

exploitation measures utilize techniques that include data mining (Moya, 2017), harvesting system logs to compare the statistical differences between the operational codes of malware and benign software (Shang, 2021), threat modeling for predictive measures across the security development lifecycle (Grimes, 2017), and continuous analysis of vulnerability information (Jiang, 2021) based on the massive libraries of data in the IoT (Jurcut, 2020).

Public Policies and Cyber Ethics

As societies continue to digitalize through the IoT (and the commoditization of data increases), there is a need to implement public policies strengthening cyber defense principles where users (both humans and machines) can retain control of their digital identities as malicious actors can masquerade as legitimate users through changing "attributes that define their identities to hide who they are" (van der Walt 2019, p. 563)**.** Effective IoT-related public policies are federated across different echelons of Government and must contain ethical considerations as the sum of its ecosystem encompasses technological innovation, users, and business processes. Ethical boundaries in the IoT carry risk as cognitive machines can manipulate data without enacting the permission consent process (Jahankani, 2020) so that distinctions between organic and synthetic entities become murky to the point where "bonds…can easily be construed as intimate" (Saetra 2019, p. 70). The data storage mediums that house digital identities are causes of concern due to "security weaknesses, dubious data-sharing and surveillance ethics, and compromised privacy rights" (Sedlmeir 2020, p. 604) while the social aspects of the IoT enable companies to "use sophisticated data operations to encourage user engagement with their networks" (Bodinger-deUriarte 2019, p. 205) through the harvesting of mass datasets to create predictive models of user behaviors (Bodinger-deUriarte, 2019). Ethical considerations within the IoT are of legal and philosophical significance as users leave digital traces of themselves as

part of the data transferal process where malicious actors can compile them to create comprehensive profiles for co-opting targeted systems through impersonation techniques using an unknowing user's credentials (Misra, 2018).

Implications for Biblical Integration

2 Corinthians 4:6 states, "He has made us competent as ministers of a new covenant – not of the letter but of the Spirit; for the letter kills, but the Spirit gives life"; Scripture speaks to the power of a covenantal relationship with God as moral absolutism governs the mutual bonding between heaven and earth as the covenant is built on trust while Thomistic tradition stipulates that "the relationship between the human and the divine was one of participation" that "specified human participation in the divine in terms of the faculty of reason" (Pryor 2006, p. 235). As beings divinely empowered with reason, we have free will to choose our paths in life including creating a secular definition of self as opposed to the Christian view of self that is anchored in the eternal nature of God's law so that there is a "centralized locus of identity, decision making, and action that serves to bind the person into a whole" (Hill 2016, p. 70). Identity-based symbiotic cybersecurity is an intertwined amalgamation of real-world and virtual influences built on implicit trust and faith expressed in seen in Luke 17:6, "He replied, "If you have faith as small as a mustard seed, you can say to this mulberry tree, 'Be uprooted and planted in the sea,' and it will obey you. The IoT alters cybersecurity dynamism as cognitive machines have become socially integrated into modern societies. Psalm 91:5 states, "You will not fear the terror of the night, nor the arrow that flies by day"; Scripture implores the protective powers of God as His knowledge enables understanding and the insight required to overcome the challenges of darkness in our lives.

Summary of the Significance of the Study

Machine cognition and the social IoT replicates societal concepts which have significant influence on physical and digital world dynamics. This quantitative study examined the complex nature of modern cyber threats to propose the establishment of cyber as an interdisciplinary field of public policy initiated through the creation of a symbiotic cybersecurity policy framework. Identity-based cognitive machine symbiotic cybersecurity policies support the interactions between the virtual and physical worlds as "the information transmitted…and exposed to the public is highly likely to be tampered with, stolen, and interfered with" (Li 2019, p. 1), particularly as the adaptative characteristics of malicious actors enable them to "modify and steal…sensitive data as well as…damage the target system" (Sharma 2017, p. 598). The very definition of self might have to be re-evaluated as the digital self of machines starts to reach parity with the digital self of humans. If cognitive machines truly become self-aware, then their social and behavioral connections with us and each other within the IoT requires that our cybersecurity policies transition from an implicit trust model to a verified trust one to preserve the integrity and legitimacy of digital exchanges. The modern malicious actor represents a transition of the cyber threat from criminal mischief to a power projection platform that weaponizes data and data exploitation to achieve specified adversarial objectives. Maintaining cohesive and persistent vigilance in the IoT requires an evolution of cybersecurity policies adapted for a behavior-based threat paradigm where malicious activities are hidden behind legitimate digital transactions and distributions, social media interactions, or camouflaged as disassociated cybercrimes.

CHAPTER TWO: LITERATURE REVIEW

Overview

In the Information Age, the IoT enables adversarial organizations (both stateless and state-sponsored) to leverage technologies in a myriad of ways to organize, plan operations, and gather sponsors and supporters. Malicious threat actors fuse the art of adaptive human behavior with the science and tools of cyber intrusion for deliberate exploitation through the interconnected nature of contemporary societies. These actors are disciplined entities that can dynamically scale based on continuous process improvement and are committed to thorough preparation and reconnaissance before executing an exploitation operation. The first part of the literature review focused on human-machine concepts, architecture of the IoT, and the presence of artificial intelligence and machine learning. The second part of the literature review focused on aspects of self-sovereign identities (SSIs) and some of the technical details involved in establishing SSIs. The gap in the research body of knowledge is the cognitive pairing of humans and machines for cybersecurity where their digital identities are components of a common humanistic policy framework incorporating social and behavioral norms. For humans to understand (and collaboratively work with) our machine partners, we need to expand the body of research into how our digital identities are mutually shaped both technologically and behaviorally.

To map relevant literature, a set of keywords were defined to evaluate the literature in the proper context. The keywords chosen were a combination of cyber policy, human-machine, teaming, AI-enabled cybersecurity, artificial intelligence, Big Data, blockchain, correlational analysis, cybersecurity policies, data-centricity, data-centric security, data exfiltration, decentralized identifier, digital trust model, distributed ledger, identity-based cyberattacks,

Internet of Things, machine learning, self-sovereign identities, and verifiable credentials. ProQuest, the Jerry Falwell Library at Liberty University (www.liberty.edu/library), the Institute of Electrical and Electronic Engineers (www.ieee.org), and the National Institute of Standards and Technology (www.nist.gov) were the primary research and data repositories used to search for authored publications, scholarly journals, and technical reports. The Falwell Library also accessed direct publisher sites such as Springer (www.springerlink.com) and O'Reilly (www.oreilly.com) for specific publications that the library URL would redirect towards. The relevant literature spans the tenets of the IoT, the data-centric nature of digital identities, the paradigm of user-controlled digital uniqueness, and data theft mitigations.

Conceptual and Theoretical Framework

Theoretical Framework

Self-determination Theory (SDT) is an "empirically based, organism theory of human behavior and personality development" (Ryan and Deci 2017, p. 3) examining the biological, social, and cultural conditions that enhance or undermine inherent human capacities (Ryan, 2017) "for psychological growth, engagement, and wellness" (Ryan 2017, p. 3). The three basic psychological needs of SDT are autonomy, competence, and relatedness (Ryan, 2017) where autonomy is the "need to self-regulate one's experiences and actions" (Ryan 2017, p. 10). Self-endorsement characterizes autonomous behavior and aligns with the interests and values of the individual (Ryan, 2017). SDT is applicable in the IoT as the persistent flow of data (and technological innovations) have enabled access to alternative worlds that "enhance or catalyze meaningful psychological experiences" (Ryan 2017, p. 509) to construct an alternative, digital identities based on motivational need or intent rather than physical attributes. This motivational element characterizes the nature of cognitive machines as they are brought online to fulfill

specific needs, wants, or objectives on behalf of a physical world increasingly dependent on the virtual one whose "design features, narratives, feedback, and goal structures…afford multiple and potent need satisfactions" (Ryan 2017, p. 511). The IoT facilitates behavioral relatedness as humans can connect with or feel helped by (Ryan, 2017) cognitive machines. Innovative applications such as *Alexa* or *Siri* have revolutionized how humans relate to their devices to the point where humans refer to these cognitive machines in the first person; modern societies that are connected to the IoT have adopted the cognitive machine as interactive partners that either directly or indirectly influence the intrinsic motivation of humans in the physical world. The increased cognition and operational autonomy of machines pivot the application of SDT towards the identification and assessment of intra-system and inter-system influences on machine behaviors as these technologies collect, process, and digest data to assemble their own digital identities, enable adaptive support to daily routines, and facilitate ML so that machines can operate independently of human input. Cognitive machines sense and comprehend their environments through passive and active interaction with data analogous to play activities characteristic of animal. Those activities expand "competencies and capacities" (Ryan 2017, p. 123) through exploration and manipulation of things as part of cognitive development.

Cognitive Evaluation Theory (CET) is a subset of SDT postulating that negative experiences to an individual's sense of autonomy and competence will diminish intrinsic motivation (Ryan, 2017) while positive experiences of the same "will enhance intrinsic motivation" (Ryan 2017, p. 124). As CET is focused on the context of relational security (Ryan, 2017) that is enhanced through "a sense of belonging and connection" (Ryan 2017, p. 124), it translates into cognitive machines behaviorally interacting and influencing each other through their connections in the IoT. ML algorithms "learn from data and improve from involvement

without any human intervention" (Agrawal 2020, p. 190) to the degree that multi-agent learning has enabled machines to collaboratively build more complete learning models together than what a single machine could produce "based on knowledge of autonomy" (Agrawal 2020, p. 194). In this example, the collaborative machines "distinguish catalogs and data sets, emphasize mutually sensed data, and edit the mistakes in the data" based on an intent to adapt to a changing environment (Agrawal, 2020). Advancements in ML have led to the application of deep learning that involves "the training of large artificial neural networks" (Agrawal 2020, p. 187) that permit machines to imitate human motion, self-navigate, collaborate through automation, conduct self-recovery without human intervention, and perform self-repair (Agrawal, 2020). Cognitive machines express autonomous behavior that is reflected in their ability to adapt to external stimuli, form problem-solving cooperative teams, and communicate with each other without human prompting; ML is transitioning the machine from an industrial tool under human control to a self-actuating partner within human societies capable of expressing autonomous self-motivating behaviors. Strengthening (and preserving) the digital identities of humans and machines in the IoT is a positive reinforcement contributing to an increase in the trust model as users gain confidence in the reputation, integrity, and resiliency of the technology ecosystem. This positive reinforcement aids in the mitigation of IoT authentication ambiguity stemming from "the lack of precision in the information regarding the subject requesting to authenticate in the system" (Dehghantanha and Choo 2019, p. 65) as the profile of a subject's successful and unsuccessful access requests (Dehghantanha, 2019) is a "metric to calculate its trust value" (Dehghantanha 2019, p. 65). The more times a subject can legitimately authenticate their identities in the IoT, the higher their trust value in a reputation-based engine as it is formed through "cumulative knowledge about the past behavior of a subject" (Dehghantanha 2019, p.

65). Negative reinforcement (in the form of digital and data exploitation) has the opposite impact as it diminishes the perceptions of digital autonomy and competence. CET contributes to behavioral assessments as the perception of free choice partly influences individual motivation. Interactions within the IoT are an aggregation of individual activities mimicking interpersonal and intrapersonal processes in the physical world facilitated through data transference, which is the core of H2H, H2M, and M2M interactions. The cleanliness of data impacts the behaviors of cognitive machines as compromised or corrupted data can either degrade the machine's functionality or expose it to malicious actor exploitation. Identity-based cognitive machine symbiotic cybersecurity policies reflect the growing connections between social behavioral models and technical governance as machines have become collaborative (and communicative) partners due to the IoT.

Conceptual Framework

The IoT enables malicious actors to exploit and weaponize data in a disciplined manner where their attacks and intrusions are increasingly executed according to the phases of the cyber kill chain. Those phases are reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives (Ju, 2020). The digitalization and datafication aspects of the IoT extend the adversarial characteristics of human behavior into the virtual environment; this behavioral element is a critical point of consideration as malicious actors are increasingly professional in executing intrusion tactics and techniques based on the intended accomplishment of organizational strategic objectives rather than operating as random isolated pockets of criminality. The People's Republic of China (PRC) case and its sponsorship of malicious actor groups lend relevance to this supposition as the patterns of behavior associated with these groups are linked to Chinese geostrategic objectives. The perspective of the Chinese

Communist Party (CCP) is that disparities in cyber capabilities prevent the PRC from "achieving information dominance and denying adversaries the use of the electromagnetic spectrum" (DoD 2020, p. 61) necessitating the seizure of strategic initiative (DoD, 2020) to enable the PRC to return "to a position of strength, prosperity, and leadership on the world stage" (DoD 2020, p. 9). Modern cyber defenders must establish a basis for behavioral pattern analysis to formulate detection models to shorten the persistence of malicious intrusion activities and lessen the harmful impacts on targeted digital environments. Coupling behavioral analytics with federated identity management establishes a baseline "through patterns or fingerprints" (Martin 2021, p. 1) where those fingerprints are assessed against specified user credentialing policies for authentication (Martin, 2021). Identities are an expression of self whose integrity is analogous to a "person's uniqueness or individuality which defines or individualizes him as a particular person and thus distinguishes him from others" (Kulhari 2018, p. 29). In the IoT, a cognitive machine occupies the same echelon of stringent trust-based credentialing and access management governance (with similar policy structures) as human users. The decentralized and distributed nature of the IoT possesses native cybersecurity vulnerabilities since its public architecture makes data "accessible to various organizations and domains across the Internet" (Khan 2020, p. 10). IoT devices operate in environments that "make data integrity a concern" (Khan 2020, p. 10) due to the lack of an assured governance structure managing the authentication and verification of user identities. Preventing malicious software exploitations requires cybersecurity policies providing governance and business process consistencies to ensure shared understanding regarding the mechanics of creating digital identity protocols and the inheritance of trust. Implementing these policies is a data-centric enabler of digital fingerprinting to establish unique characteristics that regard the cognitive machine as an equal

partner in cybersecurity rather than a tool. The ease of IoT data-sharing necessitates this change in perspective as HMT creates an equal partnership between humans and cognitive machines within the IoT.

Significance of the Concept

The IoT represents a complex technical and behavioral ecosystem digitally replicating the social dynamics of the physical world. Enhanced AI and advanced ML are enabling the cognitive machine to establish a presence bordering on individual personas where H2M and M2M communication resembles human sociological constructs. Current cybersecurity policies are highly technical and contain minimal to no considerations for the influence of machine social dynamics as the machine (cognitive or otherwise) is considered an instrument or tool rather than an independent thinking partner. Identity-based cognitive machine symbiotic cybersecurity policies are a proposed shift to an interdisciplinary approach to cybersecurity policy design coupling technical methodologies with behavioral (and social) sciences to leverage HMT for cybersecurity purposes. Human-cognitive machine digital identities should be constructed (and secured) through shared understanding that HMT partners must be able to distinguish each other within the IoT data landscape. Prevention (or mitigation) of data tampering and illicit harvesting is actualized in the IoT through the cooperative power of the HMT and the strengths of each partner.

Cognitive machine SSIs are a countermeasure for data tampering via the exploitation of legitimate digital identities. The SSI permits cyber defenders (humans and machines) to pinpoint alterations in data elements and crosswalk those alterations back to the source. Bhattacharjee (2018) postulates that the convergence of the physical and cyber worlds “translates to managing operations thousands of miles away, preventing critical machine failures through proactive

detection and remediation, digitally tracking the supply chain, providing elderly care remotely, and many similar use cases" (Bhattacharjee 2018, p. 11) where the IoT creates an ever-present attack surface that has become increasingly multi-vectored and multi-layered. As data is the core of the IoT, cybersecurity policies must concatenate cyber defense mechanisms and processes to govern humans and machines within the same paradigm so that "relevant legal and ethical requirements…to guarantee the delivery of trustworthy decisions" (Janssen 2020, p. 1) are applied.

SolarWinds SUNBURST as a Historical Example

In December 2020, the cybersecurity firm FireEye posted a public notification blog that detailed a sophisticated attack gaining unauthorized access to the organization's custom security testing tools (Seljan, 2020). Through the subsequent analysis and remediation process, multiple incident responders discovered a complex malware hiding inside a software suite from SolarWinds Corporation (a developer of IT management software and services) executing a global digital supply chain exploit leveraging "the update mechanism of its Orion platform to deliver a backdoor Trojan tracked as SUNBURST" (Seljan 2020, p. 86). SUNBURST illustrates the vulnerabilities associated with the interdependent nature of the IoT as the complexity of its digital environment requires that a user "trust the vendor of the operating system running on our machine" (Seljan 2020, p. 87) as software updates are automatically installed and security tools operate with privileged access to sensitive data and functions. In a digital supply chain exploit, malicious actors attempt to "damage government agencies and economic operators by targeting elements at any levels in their supply chain" (Seljan 2020, p. 87) particularly if the vendor or software developer is trusted. In a separate incident, Cisco Systems (a multi-national conglomerate with an extensive technological product and services portfolio) revealed that their

popular *CCleaner* software (used for routine system maintenance) was installed 2.27 million times before Cisco discovered a malicious payload buried within its code (Seljan, 2020) that severely impacted its customer base. The SUNBURST backdoor was deployed through a routine update with a digitally signed dynamic link library (DLL) module that was "loaded by the legitimate SolarWinds.BusinessLayerHost.exe of the Orion Platform software" (Seljan 2020, p. 90) that enabled the trojan to communicate with third-party servers and run during legitimate inventory checks (Seljan, 2020) with a specified targeting profile. After confirming that the victim machine was connected to a domain, SUNBURST generated a unique identifier for the victim and invoked an update loop that established a beacon between the victim and the malicious actor's command and control servers (Seljan, 2020) that permitted "internal reconnaissance, persistence, and data exfiltration" (Seljan 2020, p. 91). The malware was so sophisticated that it masqueraded its beacon as legitimate network traffic, conducted data storage with original configurations to blend in with application activities, and autonomously utilized "extensive blocklists to avoid forensic and anti-virus tools" (Seljan 2020, p. 91).

To further complicate circumstances with SolarWinds, FireEye analysts uncovered a secondary malware (tracked as SUPERNOVA) during their investigations into SUNBURST. SUPERNOVA is unrelated to SUNBURST but is a similar persistent backdoor trojan that enables "on-the-fly compilation and in-memory execution of arbitrary.NET code" (Seljan 2020, p. 92) that malicious actors supplied through remote access to trick the victim machine into executing malicious codes (Seljan, 2020). SUPERNOVA was injected through an authentication bypass vulnerability within the Orion Platform where a malicious actor could use remote access to execute commands that tricked the Orion server into processing a request "without requiring authentication" (Seljan 2020, p. 93). During their technical analysis, the cybersecurity firm

CrowdStrike discovered the SUNSPOT malware that was the vehicle used to covertly inject SUNBURST into the Orion Platform (Seljan, 2020). SUNSPOT monitored the compilation processes of infected machines running the Orion Platform and smuggled SUNBURST through a source file replacement (Seljan, 2020) so that the "code was properly inserted and remained undetected" (Seljan 2020, p. 93). Aside from autonomously extracting command line arguments to discover directory paths within Orion, SUNSPOT also could add an MD5 hash verification check "to ensure compatibility with the original source" (Seljan 2020, p. 94) so that the source code looks unaltered despite the inclusion of the SUNBURST trojan. Though the true impact of SUNBURST is still under continuous assessment and analysis, it serves to reinforce the importance of identity-based cyber resiliency paradigms as the IoT enables complex autonomous malware to exploit the persistence of the digital environment through the routine processes that modern societies have come to trust as part of normal technological functions.

Definitions

Terms deemed critical to facilitating understanding within the current study are defined along with potentially unfamiliar or ambiguous terms.

1. *Decentralized Identifiers* - A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically (W3C, n.d.)
2. *Distributed Ledger* - A non-centralized system for recording events (W3C, n.d.)
3. *Identity* - A set of attribute values (i.e. characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity (NIST, n.d.)

4. *Internet of Things (IoT)* - A network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information (NIST, n.d.)
5. *Non-person Entity* - An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts (NIST, n.d.)
6. *Person Entity* - A person or entity with authorized access (NIST, n.d.)
7. *Representation* - Information that is intended to reflect a past, current, or desired state of a given resource, in a format that can be readily communicated via the protocol, and that consists of a set of representation metadata and a potentially unbounded stream of representation data (W3C, n.d.)
8. *Self-sovereign Identities* - Identity which a user has control over without having to use a central network (W3C, n.d.)
9. *Universal Resource Identifier* - A uniform resource identifier, or URI, is a short string containing a name or address which refers to an object in the "web" (NIST, n.d.)
10. *Verifiable Credential* - A standard data model and representation format for cryptographically verifiable digital credentials (W3C, n.d.)

Related Literature

Cyber Policies

Yi (2023) expounds on the concept of the "human-centeredness" theory (Yi, 2023) of public policy where the human controls "the policy world with the aid of his policy capacity…to create and deliver public policy" (Yi 2023, p. 116). This perspective of "human-centeredness" is predicated on the idea that "human belief and cognition…have been used to determine what

methods are sensible and reasonable" (Yi 2023, p. 9). Human cognition drives the formulation of public policies and their associated disciplines as humans have long been the sole cognitive actor based on mankind's "intellectual and physical commanding power and dignity" (Yi 2023, p. 143). The digital public square (facilitated through the IoT) is a technological manifestation of self-expression as "an inalienable right encompassed within the liberties bestowed unto citizens in a democratic society" (Fowler and Maranga 2022, p. 54). This capability to self-express lies at the intersection between cyber and public policy as the ability to preserve the free flow of digital data and information influences cybersecurity public policies on a global scale (Fowler, 2022). Margetts et al (2021) state that that goal of public sector policymaking is "to influence social behavior and shape the world outside" (Margetts et al 2021, p. 163). As "technologies are completely intertwined with every act of authority" (Margetts 2021, p. 165), policies related to the digital world must account for the sociological dynamics that form the core of public policy designs and intent both for the social IoT (which include cognitive machines) and the influence of the IoT on the physical world.

Transition from "human-centeredness"

Yi (2023) argues that humans are one set of actors that reside in "a society of symbiosis between humans and non-humans" (Yi 2023, p. 118) when it pertains to the modern world that we reside in. This human-centric approach to public policies isolates cyber to technical practitioners as the issues "first require physical world insight to be developed and…codified social science knowledge of that aspect has yet to catch up to and inform the technological imperatives" (Austin 2021, p. 103). Cyber (the IoT specifically) is a complex socio-technical system (Austin, 2021) that challenges our perception of human cognition being the foremost influence on policies that govern the conditions, function, and relationships within the digital

world. Austin (2021) expounds that "the social mechanisms of disseminating knowledge have become profoundly disturbed by the information age" (Austin 2021, p. 124) as current policies do not account for the socio-political context of cyber activities nor the effects of influence, persuasion, and manipulation (Austin, 2021) in the digital world.

Human-Machine Teaming

Human-Machine teaming (HMT) is a paradigm shift in the relational and social interactions between humans and machines as digital entities within the IoT. Foundationally, HMT is the "efficient and effective integration of humans with complex machines" (Ozkaya 2020, p. 4) where both parties are equal participants in the relationship. As technological innovations continue to expand the capabilities of machine learning, humans are increasingly collaborating with machines as intelligent partners (Schadd et al, 2022). In the IoT, members of an HMT share the same data and information processing capabilities though each member has different degrees of intelligence and background awareness of the other's activities (Schadd et al, 2022). These degrees of difference prompt the necessities of communication and interdependence between the physical and digital worlds as effective HMT is reliant on the replication of human social constructs adapted for the IoT. The motivations for HMT are driven through "the need to make decisions faster, more accurately, and more safely than can humans alone" (Lawless 2022, p. 3). The IoT increases the speed of data transactions, that when coupled with its voluminous libraries, exceeds the cognitive processing capabilities of humans. HMT is a pairing of the cognitive capabilities of humans and machines for the purposes of achieving common purposes and goals.

Interdependence

One of the prevalent misconceptions of HMT is that the machine is present to compensate for human limitations with the intent to replace the human (Johnson and Vera, 2019). Technologies in the IoT function best when paired with human social constructs and processes as this interdependency requires "the knowledge of the coordination needs and possession of the mechanisms by which to achieve coordination" (Johnson and Vera 2019, p. 19). Communication, collaboration, and coordination underpin the cognitive architecture of the HMT as the concept is more than a technological pairing between the physical and digital worlds. A cognitive architecture carries "theories of psychology and understanding of intelligence" (Sun 2020, p. 19) where the basis of how the human mind learns from experiences and manifests motivations are translated into data equivalencies so that the machine can participate in equal partnership. The behavioral science aspect of cognitive architecture implies that cognitive machines can not only exceed their original programming, but that software design must account for human traits such as ethical (and moral) frameworks into technological engineering and programming. In HMT, the cognitive machine is in possession of agency defined as "the capability and authority to act autonomously in support of one's teammate" (Lyons and Wynne 2021, p. 2). This is a critical component as it stipulates that neither partner in an HMT conducts actions that are detrimental, nor adverse, to the other. Trust then becomes the anchor determining the feasibility of the HMT model.

Trust

Trust represents the fundamental aspect of managing the complex relationship within an HMT (Sapienza et al, 2022) as technological entities could possess a wide range of characteristics defining their trustworthiness (Sapienza et al, 2022). Trust dynamics are predicated on the ability of each member to communicate effectively with each other and the

strength of their relationship. Aside from sharing the belief that both partners in an HMT are performing in the interest of the other, trust also involves the "willingness to admit mistakes and accept feedback" (Demir et al 2021, p. 696). This implies that the cognitive machine does not simply accept human input (in the form of task requests) and return an output but that it is an interactive partner with shared interests, experiences, and capacities as its human partner. It is through those shared traits that the HMT learns to function as a singular entity within the IoT as "the next generation of software-intensive systems will be taught instead of programmed…" (Michael 2021, p. 106). Applied social behavioral models for the cognitive machine becomes an imperative as increasingly complex machine learning algorithms could create future circumstances where the machine "develops subjective states that allow them to monitor and report on their interpretations of reality" (Lawless et al 2019, p. 8). Social behavioral models (particularly those related to morals and ethics) gain prominence as we consider that trust in a unified HMT is contextualized when the machine learns both what it is supposed to do and "what its human teammate is supposed to do" (Lawless et al 2019, p. 9).

Trust dynamics is researched in two HMT use cases from the works of Henry et al (2022) and Ganesh (2020). Henry et al (2022) investigated the adoption of ML for clinicians to improve upon the standardized clinical case decision-making process. Specifically, their research theorized that barriers to the adoption of ML for clinical purposes are due to the "struggle to develop trust with ML-based systems" (Henry et al 2022, p. 1) and the perception that ML cannot add value to human expertise (Henry et al, 2022). The authors stipulate that where clinicians found success in incorporating cognitive machines were situations where the machine was not a tool or automation but a partner (Henry et al, 2022). Providing better quality care and case decisions with cognitive machines came about when clinicians learned to leverage the

strengths of both HMT partners (Henry et al, 2022). The use case is relevant for this study as identity-based cognitive machine symbiotic cybersecurity policies are designed from a partnering perspective where HMT partners collaborate (and communicate) to secure the IoT specifically if partners can recognize and distinguish each other's digital identities.

Ganesh (2020) investigated the social, cultural, and philosophical aspects of autonomous vehicles and their relationship with human drivers. The author stipulates that autonomous vehicles are "distributed data infrastructure running AI technologies" (Ganesh 2020, p. 2) that are in-partnership with their human counterparts and that errors in driving are due to lack of communication and coordination in handing over driving responsibilities between the human and the machine. The core premise of the research is that there is a philosophical difference between automation and autonomy as the autonomous vehicle resides in a "cognitive, data-based state" (Ganesh 2020, p. 4) with metrics, heuristics, algorithms, and quantifications of "human affects and bodies" (Ganesh 2020, p. 4) associated. The author argues that increasing the safety of autonomous vehicles means investigating the social aspects that exists between the cognitive AI and the human driver where the partner pair understand how the other acts and thinks to avoid confusion and potential conflict during the act of driving. The use case is relevant for this study as an example of the modern social dynamism that exists between the physical and digital worlds as cognitive machines can interact with their human partners through a physical medium. The IoT is present within autonomous vehicles as part of their cognitive state is enabled through internet connections. These vehicles have digital identities as the car itself is simply a chassis (or "skin") that wraps around the cognitive machine's true self which is the AI underneath. As cognitive machines become ubiquitous in the physical world, identity-based cognitive machine symbiotic cybersecurity policies gain a different degree of prominence to prevent (or mitigate)

the possibilities that malicious threats can illicitly conduct operations through physical devices or sabotage their physical functions.

The Internet of Things (IoT)

The IoT is a concept of data and information sharing with an evolving family of technologies and practices to handle, analyze, and automate the connected digital ecosystem (Tsiatsis, 2018). Fundamentally, data sits at the center of its multi-layered, multi-component architecture that "can be seen as a dynamic distributed network of smart things to produce, store, and consume the required information" (Iqbal et al 2020, p. 4) functionally enabled through data creation, communication, aggregation, and analysis (Iqbal et al, 2020). Data connectedness powers the IoT as the expanding reach of wired and wireless networks creates user communities across human societies requiring innovative approaches to technical infrastructure that incorporates an increasing reliance on automation. The transformational effect of digital technologies has a societal impact as automation becomes smarter, self-sufficient, and an active participant in data exchange through H2M and M2M interactions. The algorithms of the IoT digitize the concept of self that impacts the "who" and "how" societies interact as contemporary users are comfortable conferring with their smartphones and self-driving cars, collaborating through social media software applications, and utilizing virtual reality devices where the interaction is dependent on data transactions. The digitalization of modern societies has led to the creation of cyber-physical systems integrating physical and computing domains (Aloqaily et al, 2022) where "emerging technologies will disrupt for good or ill how we live, work, and even think" (Bloom 2020, p. 4) as humans continue to incorporate cognitive machines into their routine activities. Whether it is a dependence on a social media platform to monetize human interaction, propagation of a cloud environment to connect users to their data anywhere in the

world, or using digital assistants to navigate, translate, or execute “hands-free” device functionality, the IoT is an element of modern societies that have embraced its ubiquitous nature. As the digital world melds with the physical, modern cyber defense must embed security into every facet of the IoT environment as Alenezi et al (2020) explain that the current evolutionary cycle of malware has witnessed its transcendence into weaponized platforms focused on virtual espionage (Alenezi, 2020).

Artificial Intelligence

Contemporary human actions and cultural practices take place within the “context of complex, powerful technological and social systems” (Elliott 2019, p. 49) as digitization is auspiciously replicated to create a digital data economy intertwining over 3 billion people (Elliott, 2019). The rising tide of automation and AI is both transformative and disruptive as the promises of innovation, productivity, and economic growth through the digital revolution (Elliott, 2019) are counterbalanced by a datafication effect where who we are is “made, read, interpreted, and intelligible according to data” (Cheney-Lippold 2017, p. 32) that is prone to external influences of subjectivity. Maleh et al (2021) define AI as “any system perceiving its environmental state and taking action to increase its chances for success” (Maleh et al 2021, p. 17) whose evolution is due to “large-scale development and knowledge generation through sensing systems, IoT devices, social media, and web applications” (Maleh 2021, p. 5). The market potential of AI is estimated to reach $13 trillion by 2030 (Maleh, 2021) and is intimately linked to data as ML grants the AI “the ability to learn automatically and gain experience without pre-programming” (Sinha 2019, p. 117) as the AI concentrates on data that needs to be accessed to make the system learn on its own (Sinha, 2019). The datafication effect and the propagation of ML are what enable automation to scan, process, and analyze the massive amounts of created

data as societies continue to become digital (Dey, 2020). ML and the IoT converge in the field of data analytics as ML-based algorithms process the massive volumes of raw data in the IoT through "data aggregation, data summarization, mathematical logical operations, data mining" (Adi et al 2020, p. 16207) to create actionable insights through analytical modeling as ML techniques can support continuous assessment of vulnerability data sources to manage the burden of analyzing vulnerability information (Jiang, 2021).

Security Challenges

As the IoT is not a monolithic construct, the data that traverses it must navigate through a multitude of nodes to reach its destination; each node must maintain the proper encryption capabilities and mechanisms (Khan, 2018) to ensure its confidentiality. Yet, due to the diverse nature of the IoT, "data stored on a device is vulnerable to privacy violation by compromising nodes" (Khan 2018, p. 397) as each component (and the data itself) presents a potential attack surface for malicious actors. Vadiya et al (2020) note that "dependability is an essential property of IoT devices" (Vadiya 2020, p. 189) due to the presumed trust inherent within the IoT that devices and their transmitted data are legitimate. Yet, as malicious actors have cloned or counterfeited devices (Vadiya, 2020) to function in place of legitimate ones for illicit operations, it becomes imperative that modern cyber defense techniques account for the identities of the devices and systems forming the core of the H2M and M2M data interactions. Cirani et al (2018) summarize the security challenges within the IoT as the unauthorized cloning of smart objects, malicious substitution of smart objects during installation, firmware replacement, extraction of security parameters, eavesdropping, man-in-middle cyberattacks during data exchanges, routing attacks, denial-of-service attacks, and privacy threats (Cirani, 2018). Across the spectrum of IoT devices, the availability of computing resources and degree of power

consumption constrains the implementation of "traditional security mechanisms such as SSL/TLS" (Mustafaev 2020, p. 1) thus triggering the need to become more innovative in identity verification to ensure reliability. As identity can be considered the sum of attributes (Pal, 2018), an innovative approach is to consider the partial identities of each component attribute as a source of unique identifiers that would link together to "create an identity model that serves applications and policy specification needs" (Pal 2018, p. 50). This aggregation model is analogous to the physical identities of humans as an aggregation of characteristics associated with our hair, eye, and skin colors plus height and weight. An aggregation model for assembling digital identities reflects how DIDs are an attribute inside the credential metadata of VCs as the unique identifier is aggregated with other characteristics unique to cognitive machines so that the VC is a compilation of multiple data fields comprehendible to other cognitive machines in M2M exchanges. VC is a composite architecture for the cognitive machine much like how a driver's license is a composite of the unique traits identifying a human in the physical world. Identity-based symbiotic cybersecurity policies must account for the unique identifying traits of cognitive machines. In the IoT, these traits are expressed as data and data attributes thus circling back to the primacy of data and how malicious actors seek to exploit them.

The requirement for innovation extends to virtualized infrastructure as cloud computing gains prominence as an IoT enabler. The National Institute of Standards and Technology defines the cloud as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mitra and Gofman 2016, p. 246). The backbone of the cloud is the virtual machines that can run multiple operations on a single physical machine while sharing "all hardware resources" (Sinha 2019, p. 26). Virtualization carries risk as the hypervisor (which is the logical bridge connecting the virtual machines to their

physical hardware) is a single point of failure from a security perspective (Sinha, 2019) as malicious actors can hijack a hypervisor to "acquire complete control of a server" (Sinha 2019, p. 26). These intrusion techniques are based either on the acquisition of legitimate credentials or the forging of the same that malicious actors use to conduct their initial reconnaissance of a target environment specifically through the monitoring of data flow to determine systemic ingress points.

Big Data and Cybersecurity

Traditional approaches coupled with human analytics are unable to manage the complex dynamics of the modern IoT (Rawat et al, 2021) as the enormity of the data landscape makes it difficult to know (much less mitigate) the threat (Rawat, 2021). A critical aspect in defining the IoT as an innovative paradigm is the smartness of its "services and applications where devices are capable of automatically capturing data for analysis" (Chae 2019, p. 3). This elevates the need to maintain confidence as "the necessity to identify (and eventually trust) who we interact with" (Moallem 2019, p. 51) will continue to grow as the IoT continues to propagate. The increasing smartness of the IoT creates unique security vulnerabilities as its interconnected devices and digital objects "have the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" (Mahmood 2018, p. 19) as digital transformation takes traditional processes and integrates them with automated data flows to create intelligent information and operational technologies (Moller, 2020). It is estimated that the total volume of digital data increased to "40 trillion gigabytes in 2020" (Ullah & Babar 2022, p. 1) and the amount analyzed "jumped from 0.5% in 2012 to 37% in 2019" (Ullah 2022, p. 1) with 97.2% of contemporary organizations investing across the spectrum of big data architecture (Ullah, 2022). The concept (and lingo) of big data continues to be enculturated into

contemporary societies as Internet capabilities are extended through terrestrial cellular networks, satellites, and underwater telecommunication cables. The extension of the internet enables the ease of data transference residing at the core of the IoT necessitating the requirement to secure both the devices producing and consuming data and the "nodes through which the data is transmitted or stored" (Mahmood 2018, p. 23).

Big Data Analytics

Big data is the nomenclature that permits an organization "to have access to a large amount of information, normally unstructured" (Maleh 2019, p. 52) which it previously did not have the capability (or capacity) to access. Big data represents a fundamental shift in how societies (and organizations) collect and use information where the interconnectivity of the IoT combines data processing capabilities with rapid analytical velocity (Maleh, 2019). This combination has steadily eroded the effectiveness of passive cyber defenses that include virus detection, firewalls, patches, and threat detection (Wang and Jones, 2021) in favor of active defenses synchronizing real-time capabilities to accomplish "detection and forensics, deception, and attack termination" (Wang 2021, p. 410). The estimated 4.57 billion users connected to the Internet generate over 2.5 quantillion bytes of data daily (Alani, 2021) where "Instagram users upload an average of 95 million photos and videos per day" (Alani 2021, p. 85), Facebook publishes 510,000 comments an hour (Alani, 2021), and 156 million email messages are sent every minute (Alani, 2021). Traditional cybersecurity methodologies are state-based mechanisms and techniques focusing on the "current state of a system and how to maintain it" (Alani 2021, p. 86) as those systems are generally self-contained entities with known baseline characteristics and capabilities. Data as a threat vector is a phenomenon of the IoT due to volume and velocity as malicious actors can exploit its persistency and presence as a core

enabler of modern smart environments. Big data analytics attempts to use "advanced analytic techniques…to uncover hidden patterns, unknown correlations, market trends, customer preferences, and other useful business information" (Savas and Deng 2017, p. 4) as active cyber defense techniques tend to gravitate towards predictive analysis through data aggregation to create threat intelligence "that helps broaden situational awareness, minimize cyber risk, and improve incident response" (Savas 2017, p. 12).

Big data analytics supports the detection and prevention of malicious threats through the classification, based on semantics, of disparate data collected from multiple sources to create comprehensive linkages (Angin et al, 2019) as detecting variances in the patterns of data is foundational to modern IoT resiliency. This methodology enables the preparation, cleansing, and querying of "heterogenous data with incomplete and/or noisy records" (Rawat 2021, p. 2057) so that humans can make sense of it. Malicious actors operating in the IoT can exploit its public nature to exfiltrate data as public resources and anonymous networks provide non-attributional techniques for them to "protect the final destination of the data" (Borges 2021, p. 199). Big data analytics is a pivot of contemporary cyber defense paradigms acknowledging the critical role that data inhabits in the IoT as "the rise of polymorphic malware and other evolving threats" (Rawat 2021, p. 2056) requires an enormous amount of data to derive actionable insights (Rawat, 2021). Achieving decision advantage in active cyber defense requires innovative approaches that involve "data mining and machine learning, artificial intelligence, knowledge-based and statistical models" (Palomares et al 2017, p. 128); the sheer volume and velocity of data transference in the IoT (coupled with the complex infrastructure required to sustain its persistent digital environment) have outpaced human-derived cyber analytical techniques and methodologies.

Machine Learning

Data breaches can have a devastating economic and organizational impact with an estimated annual global loss of US$4 billion (Sarker et al, 2021) as digitalization and the IoT has enabled an exponential rise in malicious activities (Sarker, 2021). AI/ML is at the forefront of an emergent data-driven cyber defense model to "transform raw data into decision making" (Sarker 2021, p. 9) as "security is all about data" (Sarker 2021, p. 9). A data-driven cyber defense model "attempts to quantify cyber-risks or incidents" (Sarker 2021, p. 11) to enable inferential techniques to analyze behavioral patterns associated with data itself (Sarker, 2021). Human-machine collaboration forms the core of active (and adaptive) data-driven cyber defense methodologies to augment "human capacities for the execution of cybersecurity tasks" (Andrade 2019, p. 3) as humans alone are unable to collect, filter, triage, and analyze the extensive datasets associated with the IoT. Sikos and Choo (2020) diagram the threat space through an orthogonal dimensions model categorized across the three axes of motivation, localization, and agent (Sikos, 2020) as a method for establishing threat intelligence taxonomies and ontologies (Sikos, 2020). The move towards a structured framework for defining the threat is, in part, a prerequisite for creating machine-readable data models to power enhanced analytics where AI/ML both augment the human cyber analyst and progressively self-educate particularly in the construction of "predictive models for vulnerabilities classification, clustering, and ranking" (Parkinson et al 2018, p. 17). The prevalence of AI in cyber analytics and cyber defense requires a strong trust model to authenticate and preserve machine identities as the machine is trained to simulate human skills (Naik et al, 2022) with the ability to "self-direct, harmonize, diagnose, and…learn…by producing understandable knowledge from discrete data" (Naik 2022, p. 1763).

AI-enabled Cybersecurity

Access and analysis of rich data sources determine the effectiveness of AI employment for cybersecurity (Samtani et al, 2020). Internal data sources are those close to the critical assets of an organization (Samtani, 2020) that can range from physical devices (servers, databases, routes, etc.) to virtual machine images (Samtani, 2020) whose data flows and transference "contains data such as source, destination, bytes, headers, and others" (Samtani 2020, p. 3). External data sources are those located across the broader digital landscape including publicly accessible coding repositories, IoT search engines, and Dark Web platforms (Samtani, 2020); collected data assist organizations in understanding the accessibility of their code, mapping the public access points to their devices, and construct threat intelligence through the silent surveillance of social forums that malicious actors utilize (Samtani, 2020). Data is what permits an AI to comprehend and adapt to the threat environment particularly as Big Data connects it to multiple data streams and its behavioral heuristics enable it to craft a picture of anomalous behavior within a technical ecosystem "to predict human rather than just machine behavior" (Stevens 2020, p. 166) in recognition that modern cyber defense takes place at the intersection of technologies, users, and processes (Stevens, 2020). The advent of AI-enabled cybersecurity is a model that "substitutes human cognition as the arbiter of network decision-making and regulation of data flows" (Stevens 2020, p. 167) as modern cyber defenders turn to AI algorithms to conduct fine-grained pattern analysis of the voluminous data resident across the IoT (Samtani, 2020).

Enhanced Detection and Analysis

The potentiality for increasing human cognitive skills and abilities is dependent on access to data and information, the same is true of AI as the deployment and integration of intelligent

algorithms are predicated on data access to enable deep and reinforcement learning (Aloqaily, 2022). As the IoT becomes smarter and more autonomous, modern cyber defense models must employ similar smart technologies to "provide more secure and robust privacy-preserving solutions for personal and ubiquitous systems" (Aloqaily 2022, p. 2). The wealth of data in the IoT has enabled malicious actors to develop their smart tools to exploit the persistent digital environment as the rise of intelligent malware and the mechanisms of AI-enabled malicious cyber activities permits "sophisticated malware to learn about the defensive environment and compartmentalize lessons learned" (Whyte 2020, p. 26) so that it can adapt to changing mission parameters and select alternative approaches without direct command from a human actor (Whyte, 2020). Defensive AI-enabled security measures combine robust data mining, data enrichment, deep learning, and natural language processing to integrate "AI explainability methodologies and data cleaning" (Liu et al 2021, p. 10) to teach an AI data anomaly detection, proactive intrusion detection techniques, and self-constructed predictive analytics so that humans and machines alike can respond to intrusion "incidents before the actual damage happens" (Liu 2021, p. 6). Generating data structure and context is foundational for AI learning as raw, unstructured data is noisy and inconsistent (Kim and Park, 2020) thus limiting the ability of the AI to make sense of the data it is evaluating to reach conclusions and formulate insightful analysis. The persistency, prevalence, and availability of data in the IoT have made it the single most critical resource of the persistent digital environment where smart technologies (and automation) transform both cyber defense models and malicious actor activities. Increasingly, the need to employ AI-enabled threat and intrusion detection capabilities is due to the injection of AI-augmented malware to "automate the process of exploit generation, attack launch and patch generation" (Arivudainambi et al 2019, p. 50). Preserving the identities of cognitive

machines is a component of the systemic approach to increasing IoT resiliency as intelligent (and automated) algorithms harness, and harvest, data for self-propagation and dynamic adaption. H2M and M2M interactions create degrees of visibility for cognitive machines as the human user might not be cognizant of the automated agent facilitating data transferences, recording data transactions, or monitoring data flows within the IoT.

Data-centric Security

Data sits at the heart of the IoT as software applications that traffic in big data span industries such as sports, medicine, e-commerce, media, retail and sales, energy, human resources, travel, and fraud protection (Till, 2017) as business models "aggregate and analyze security data and transform it into an information product" (Till 2017, p. 173). The commoditization of data necessities a shift in our cyber defense perspective as the IoT has transformed data from being the mere output of human activities into a core component of the contemporary societal fabric as data itself carries intrinsic value thus requiring "fine-grained access control over data" (Rasori et al 2020, p. 77) as the "intrinsic characteristic of the IoT is persistent gathering and linkage of user data to provide adapted capabilities" (Demertzis 2020, p. 3) where the constant exchange of data and information establishes a persistent attack surface. The US Federal Trade Commission (FTC) estimates that individual data brokers can possess over 3000 data segments on every US consumer (Shackleford, 2020) which translates into an industry posting "$150 billion in revenue" (Shackleford 2020, p. 58) where the worth of data is in the trillions (Shackleford, 2020). This intrinsic value has made data an "attractive target for adversaries" (Bitomsky et al 2018, p. 589) that alters organizational and individual risk calculations as industrial business models shift to integrate data into products and services to meet consumer demand while individuals capitalize on the persistency of data for personal gain

or to fulfill daily responsibilities. Data-centric security is an evolution in the cyber defense paradigm that recognizes the interconnected nature between data, its producers, and consumers in the modern IoT as malicious actor attempts to harvest, manipulate, or alter data has a repercussive impact across multiple sectors.

Trust and the IoT

Hammi et al (2018) note that in the IoT, "things process and exchange data without human intervention" (Hammi et al 2018, p. 126) necessitating the importance of identity verification as a mechanism to preserve trust within the ecosystem. The heterogeneous composition of entities operating in the IoT has rendered the traditional cybersecurity methodologies of hard security through authenticated access control (Ting et al, 2021) unfeasible as a multitude of different devices (and their users) can enter or exit the IoT across time and space while malicious actors can infiltrate through the same vectors as legitimate users. This fluidity in the IoT makes the traditional approach to trust centralization difficult as centralized storage of identity attributes has expansive repercussions in the event of a breach (Moreno et al, 2021). The architecture of trust within the IoT reflects the same social properties garnered in human societies to permit "digital entities to perceive others and choose their interactions, as is done in the real world" (Ting 2021, p. 106473). The interactive architecture of the IoT replicates many of the same societal principles of human interactions in the physical world as H2H, H2M, and M2M are conceptual derivatives within the digital world. The scale of human interaction in the physical world is based on the degree of trust that users have when interacting with others (a higher degree of trust translates to a larger scale of information sharing); the modern trust paradigm in the IoT is a behavioral approach to cyber defense in recognition that contemporary data exchange incorporates more than the 1s and 0s of binary code. Dooley and Rooney (2017)

annotate an example where domain name servers (DNS) pass trust relationships between the resolver cache and the recursive servers; if the trusted data source is corrupted, the resolver cache "could inadvertently redirect the user application to an inappropriate destination" (Dooley and Rooney 2017, p. 5) thus creating an attack surface where malicious actors could "collect authentication credentials or financial information" (Dooley 2017, p. 6).

Identity

Protection of digital resources, data integrity, and data confidentiality requires that our cyber defense strategies and methodologies seek to determine the legitimacy of access requests so that resources are made available in a timely and consistent manner (Sule et al, 2021). In the digital world, identity is "what makes us unique and identical to others" (Sule 2021, p. 2) that determines what kind of transactions entities can participate in (Sule, 2021). Digital identities are critical to facilitating innovative trust-based cyber defense methodologies as identity verification is linked to the data objects and resources that users seek to access requiring a management model encompassing physical and logical objects to facilitate "efficient and fine-grained management of attributes" (Yang 2020, p. 2) associated with the components that build them. Li et al (2020) note that "data-centric authentication should be provided to support…secure data retrieval" (Li 2020, p. 16) as malicious actors endeavor to compromise both the logical and physical aspects of the IoT. Identity-based attacks are designed to permit a malicious actor to function as an electronic imposter (Haber and Rolls, 2019) to masquerade as legitimate users or change "attributes that define their identities to hide who they are" (van der Walt 2019, p. 563) in an endeavor to gain access as far down the permission chain as possible (Haber, 2019). Identity-based cyber resiliency is about preserving what makes humans and machines unique so that the integrity of the "self" does not become this point of exploitation for

malicious actors. To that extent, identity preservation is a holistic concept combining policies and governance structures with legal precedence and technological innovation to ensure that humans and machines can prove their identities in a genuine and trustable manner "without disclosing unnecessary knowledge" (Shibuya 2020, p. 89). This latter stipulation is critical as the storage platforms retaining and managing identity data are themselves points of concern "due to security weaknesses, dubious data-sharing and surveillance ethics, and compromised privacy rights" (Sedlmeir et al 2021, p. 604).

Distributed Ledger

Due to its simple implementation, the IoT is designed around a centralized architecture for data processing, unified analysis, and service delivery (Liao et al, 2021) that enables ease of control across IoT nodes. The contemporary commoditization and intrinsic value of data, though, make this centralized architecture a prime target for malicious actors; distributed ledger technologies are an emergent, innovative approach to mitigating the potential for attacks. Distributed ledger architecture permits P2P IoT nodes to manage data security through membership consensus as each independently verifies nodal identities using tamper-resistant, cryptographically signed data blocks (Liao et al, 2021). These data blocks contain valuable information associated with the data originator through indexing of "the hash value of the previous block" (Zhang et al 2021, p. 101) that is combined with the hash value and time stamp of the current block to capture data lineage and traceability to establish a cooperative authentication scheme with lightweight protocols (Tariq et al, 2019). As the IoT is ubiquitous and boundary-less where entities are "oblivious about the location where the data resides" (Felemban et al 2019, p. 41), distributed ledger technologies mandate that P2P nodes prove their identities through the exchange of credentials (Bandara et al, 2021) before engaging in data

transferals or granting access to the data contained within the network. Maintaining trust integrity is a foundational principle of a distributed ledger as "the information of the entire network transaction" (Lu et al 2021, p. 31893) is stored on a preceding block and used to verify the validity of the information transaction (as an anti-tampering mechanism) before the next block in the ledger can be generated (Lu, 2021). In this way, distributed ledger creates a virtual data chain of custody that ensures data integrity as it permits data owners to "audit their data" (Wylde et al 2022, p. 127) to discover if it has been tampered with and, if so, the data provider and the path to the tampered data can be uncovered "to disable the further spread" (Li et al 2020, p. 15) of the tampered data.

Blockchain

Blockchain is a distributed systemic model that is "based on consensus rules that allow the transfer of value between entities" (Panarello et al 2018, p. 4) that is not reliant on trusted third parties to issue credentialing certificates to validate digital identities. The need for blockchain is based on a distributed ledger principle that humans and machines own their own identities through a "democracy of computing power" (Panarello et al 2018, p. 5) derived from a "proof-of-work" concept anchored in computationally complex mathematical problems that are "hard to solve and very easy to verify" (Panarello et al 2018, p. 7) as a foundation for its cryptographic schemas. Blockchain places the burden of trust on the individual humans and machines interacting within the IoT rather than leveraging a third-party trusted agent to issue credentials as "what you write in the chain stays in the chain" (Moreno et al, 2021, p. 105789). As such, the information contained in a blockchain ledger is public and verifiable (Gulati and Huang, 2019) as the blocks themselves are updateable if the transactions are "atomic, consistent, isolated, and durable" (Seike et al 2018, p. 272).

Cryptographic Uniqueness

Blockchain can function as unique identifier registries to "store information about who is related to specific IDs and how to access information about them" (Lyons et al 2019, p. 16) as humans and machines are responsible for owning, managing, and verifying their own digital identities. Through this unique identifier management structure, blockchain requires that data owners notarize their portion of the chain using timestamps and electronic seals (Lyons et al, 2019) so that their credentials verify the integrity of the data as it is transmitted across the IoT. As stated in the previous section, this fine-grained access control over data is amplified as data owners can publish and distribute "decryption keys for data users through the blockchain" (Gao et al 2021, p. 2) thereby strengthening data integrity within the chain as the structure of individual blocks are irreversible once notarized (Ma et al, 2021) unless deliberately tampered with. Critical to the blockchain architecture is its cryptographic methodologies to ensure ledger transparency where decentralized P2P trust has scalable credibility underpin so that "the more an entity is trusted by others, the higher is its credibility" (Shi et al 2021, p. 2056) thereby providing a structural model to confirm data ownership, identity authorization, and build trust relationships to manage data access control (Shi et al, 2021). Blockchain can adhere to the precepts of data provenance that "provides information on all changes performed on data exchanged between multiple entities" (Shetty et al, 2019, p. 172) to address the ancestry of data and ensure that deliberate alterations and tampering are identifiable within the data objects.

Self-Sovereign Identities

The Sovrin Foundation (www.sovrin.org) defines self-sovereign identities (SSIs) as a "lifetime portable digital identity that does not depend on any centralized authority" (Sovrin, n.d.). Sedlmeir et al (2021) define SSI as a set of principles about digital identities, privacy

rights, and personal information (Sedlmeir, 2021) anchored in the premise that individuals should not be required to cede a disproportionate amount of control of their digital identities to centralized providers in the era of big data (Sedlmeir, 2021). As digital identities are comprised of the data attributed (and shared) inside the IoT through H2H, H2M, and M2M interactions, its construction has become multi-variate. SSI is an emergent concept that entities maintain full privileges towards the management of their own identities with the ability "to decide its correlation across different contexts without requiring any permission from any administrative authority" (Naik and Jenkins 2020, p. 3). To maintain sovereignty, an entity must exist in the real world either as a physical or virtualized entity that is independent of its digital form (Naik, 2020) to ensure that its attributes are public and accessible. SSI enables a layered authentication model that "separates cryptographic and application-specific authentication" (Fedrecheski et al 2020, p. 5) where entities first prove their identities to each other before engaging in trust verification of the data intended to be exchanged at the application level. SSI is an efficient framework for the management of human user identities as it permits "identity owners to store personal data on their own device, allowing organizations to minimize their various data management issues related to storage, cost, security, privacy, and bureaucracy" (Naik 2020, p. 2).

SSI Ecosystem

SSI is unique from previous identity models as it utilizes distributed ledger technologies to create a "cryptographically verifiable digital identity that is fully governed by its owner" (Naik 2020, p. 2). NIST defines digital identity as "the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts" (Soltani et al 2021, p.

4). The principles defining an SSI ecosystem are existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection (Soltani, 2021) built from the use of decentralized identifiers (DIDs), verifiable credentials (VCs), and decentralized public key infrastructure (DPKI) (Soltani, 2021). The DID is a critical component of the SSI model as it is a globally unique cryptographic identifier scheme generated based on key pairs and cryptographically provable through digital signatures (Soltani, 2021). DID registries ensure the uniqueness of an identity's identifier (Gruner et al, 2021) as it provides "verifiable proof of existence and revocation of an attribute" (Gruner 2021, p. 138555). The VC is an "interoperable data structure suitable for representing cryptographically verifiable and tamper-proof claims" (Soltani 2021, p. 10) based on zero-knowledge proof principles "where an entity can prove to another entity that they know a certain value without disclosing the actual value" (Fedrecheski 2020, p. 2). The DPKI is a set of services, tools, processes, and technologies facilitating the performance of cryptographic operations (Soltani, 2021). As an extension of the ecosystem, Zeng et al (2021) advocate for a persistent data structure where an identity owner generates a cryptographic algorithm with public and private key pairs, passes the public key to an identity verifier through a blockchain to link the digital and real identities, and uses their private key to sign a time-sensitive, one-time message from the verifier on the blockchain to complete identity verification (Zeng, 2021). The persistent data structure provides consistency of credibility and is designed to support large-scale digital identities (Zeng, 2021). Yuan et al (2020) argue for enhanced cryptographic key management anchored in a nodal scheme where a central node collects the location information of all other nodes within the network in advance (Yuan, 2020) to authenticate themselves to each other. The automated perpetuation schema mimics human social behaviors where a person confirms the identity of the

individual(s) in communication before exchanging information. Standards and protocols underpin SSI as the automated algorithms construct the identification schemes enabling entities to prove their identities through the "acquisition of corroborative evidence" (Chia and Chin 2020, p. 61711). The constraints on SSI are due to available computer resourcing and code-pair schematics (Chia, 2020) as fully adoptable SSI requires the ability to run asymmetric cryptography and support continuous metadata transmissions of VCs that can be over 500 bytes in size each (Fedrecheski 2020, p. 6).

Decentralized Identifiers

A decentralized identifier (DID) is composed of a string of characters designed to identify a resource (Preukschat et al, 2021) whose core properties are persistence, resolvability, cryptographic verifiability, and decentralization (Preukschat, 2021). The design of the DID removes the dependency on a central issuing party that "creates or controls the identifier" (Kortesniemi et al 2019, p. 3) as the identifier is entirely created and managed by the identity owner (Kortesniemi, 2019). Figure 1 is a simple example of a DID.

Figure 1

Simple Example of a Decentralized Identifier

Note. The image comes from the Decentralized Identifier version 1.0 core architecture, data model, and representations document from the World Wide Web Consortium (W3C) (https://www.w3.org/TR/2022/REC-did-core-20220719/)

Identifiers are used to impart “unique names to data to express its characteristics” (Kang et al 2021, p. 4) for accountability and access control (Kang, 2021). The DID holds identity owners accountable as it is their credentials that validate the identifier. The DID is sister to the VC as a pillar for SSI standardization as the DID string is an Internet Engineering Task Force (IETF) standard that is globally unique to each DID (analogous to a human fingerprint). The DID document contains machine-readable metadata about the subject that requires verification (the document can contain information about cryptographic keys, authentication methods, or other descriptors on how to engage in a trusted interaction) (Preukschat, 2021). More importantly, there is a 1-to-1 relationship between a DID and its document so once a document is cryptographically verified with a public key, any alterations to the key pair require an update using the previous private key thus ensuring a chain of trust between documents and their associated DIDs (Preukschat, 2021).

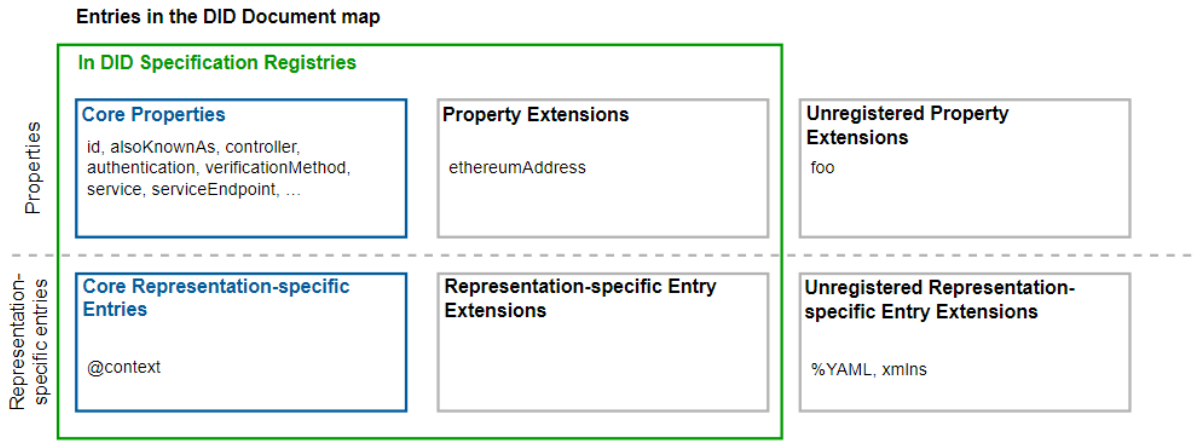
Global Uniqueness

DID documents are stored in globally accessible registries “using blockchain, distributed ledger P2P networks, or other systems with similar capabilities” (Fortiou and Polyzos 2019, p. 4). If an entity wishes to prove its identity to another entity, the verifier retrieves the corresponding DID document to extract the public key and then authenticates it through the issuance of a digital challenge that the proving entity must provide a digital signature (Fortiou, 2019). As stated in the introductory section, alterations to the cryptographic key pairs bound to the DID document trigger an update (the DID itself is not impacted) thus the DID document maintains the integrity of the record. Verifying entities retrieving a DID document from a registry are provided the most up-to-date version of the DID document thus retaining the property of revocation. The DID document is composed of a comprehensive set of elements

including the DID of the subject, the associated public keys, the authentication method, authorized operations to be performed on behalf of the subject, methods of subject discovery, document creation timestamp, and the digital signature of the subject (Omar and Basir, 2020). The machine-readable nature of the DID document metadata is an important characteristic as their maintenance and updates can be entirely performed without a human in the loop. As AI is an increasing presence within the IoT, the automated nature of DID document management maintains system integrity at the speed of computing resources particularly as DID and VCs are coupled with distributed ledger technologies to implement identity-based authentication paradigms extending beyond traditional cryptographic protocols and PKI infrastructures. Identity verification and revocation provide subject-level granularity predicated on entity uniqueness operating at scale especially as IoT components are "heterogenous in nature with self-configured properties" (Sheron et al 2019, p. 2). Figure 2 is a graphical depiction of the entries associated with a DID document.

Figure 2

Entries in a DID Document



Note. The image comes from the Decentralized Identifier version 1.0 core architecture, data model, and representations document from the World Wide Web Consortium (W3C) (https://www.w3.org/TR/2022/REC-did-core-20220719/)

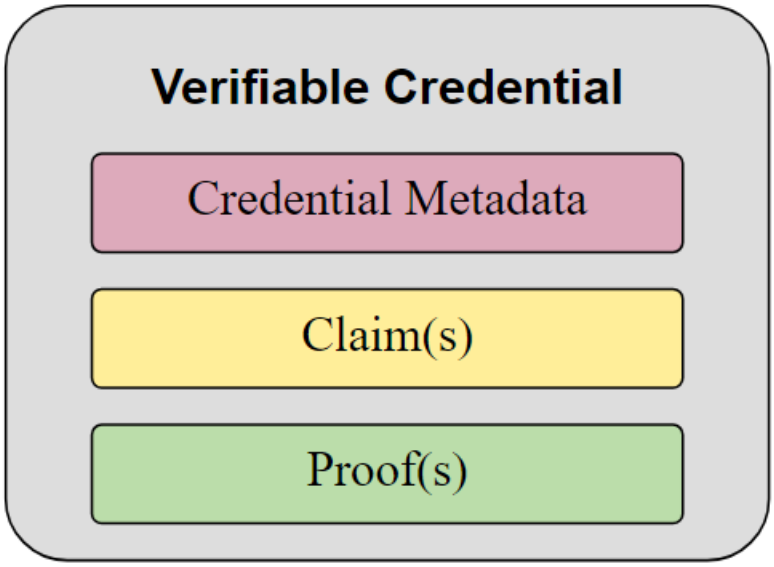
Verifiable Credentials

VCs are digital forms of common physical credentials (Preukschat, 2021) that cannot be copied or cloned, can disclose portions of verifiable data, and can be delegated to other users if the identity owner authorizes it (Preukschat, 2021). VCs form the core of the SSI architecture as their use of digital signatures makes them "more tamper-resistant and credible" (Omar 2020, p. 177) and creates an association between machine-verifiable properties and the identifier of an entity (Kortesniemi, 2019). VCs function in the same manner as driver's licenses or photo IDs to provide credible evidence of an individual's identity. The basic structure of the VC data model contains six information fields defined as context, type, ID, issuer, subject credentials, and a digital signature as proof (Preukschat, 2021) that are stored in globally accessible verifiable data registries used for "verifying the status, integrity, and freshness of a VC" (Alzahrani 2022, p. 388). VC roles within the SSI model are well-defined as the issuer of the VC notarizes its

validity (Cho et al, 2021) and the holder "acts as a real information subject who can exercise all rights to the VC" (Cho 2021, p. 1858). To maintain the chain of trust, a VC must be affiliated with a real subject to be considered true and digitally signed to be considered valid, without both aspects, the VC is not legitimate. Figure 3 depicts the basic components of a VC.

Figure 3

Basic Components of a Verifiable Credential



Note. The image comes from the Verifiable Credentials Data Model version 1.1 document from the World Wide Web Consortium (W3C) (https://www.w3.org/TR/vc-data-model/#core-data-model)

Data Exfiltration

Data exfiltration is the formal term for data theft that is an increasing cyber defense challenge as the IoT continues to propagate and malicious actors become sophisticated in their attack paradigms and methodologies. Ullah et al (2018) illustrate the impact of a data breach in October 2017 of 200 million American voters from the database of the Republican National Committee due to a flaw in database configuration exposed personal information including

"name, home address, phone number, date of birth, and voter registration details" (Ullah 2018, p. 19). There is a multitude of data exfiltration attack vectors encompassing both network-based and physical-based attacks (Ullah, 2018) where network-based vectors use existing infrastructure to steal data from individual organizations (Ullah, 2018) and physical ones are unauthorized or illegal physical access to data (Ullah, 2018). Due to its data-centric nature, data exfiltration within the IoT has compounding ramifications, particularly as network-based malware use covert channels for payload delivery (Nadler et al, 2019). A covert channel is defined as "a channel of communications that are neither designed nor intended to transfer information" (Alcaraz et al 2019, p. 3980). A vector in this method of attack is through domain name server (DNS) protocols as restrictions on DNS communications may disconnect legitimate remote services (Nadler, 2019) and the protocols themselves are "not designed for arbitrary data exchange" (Nadler 2019, p. 37). Ahmed et al (2020) document a common method of DNS exploit where malicious actors register a domain, then embed malware in a host that encodes "valuable private information…into a DNS request, sends the request to the authoritative name server in the malicious domain that sends a response back to establish "a low-rate but covert two-way communication channel" (Ahmed 2020, p. 265). The malicious actors exploit legitimate data exchange protocols as the "decentralization of the DNS allows any user to configure the authoritative name server for their domain names" (Nadler 2019, p. 38). DNS exploitations are insidious as the data exfiltration occurs in segments (or packets) where the full data content is assembled on the malicious server side (Steadman, 2021).

Advanced Persistent Threats

Advanced persistent threats (APTs) are a continuous long-term presence that adapts and maintains the appropriate level of interaction to achieve their objectives (Al-Matarneh, 2020)

because each intrusion is “customized and designed to the systems” (DeVore 2017, p. 41) targeted for intrusion and exploitation. The NIST defines an APT as “an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors” (Dehghantanha 2019, p. 226). The advanced capabilities of an APT preclude the implementation of the static, bastion-based methodologies of traditional cybersecurity measures as their non-targeted nature does not possess the dynamic flexibility required to mitigate the adaptability of these malicious actors. Chen et al (2018) state that traditional firewalls and anti-viruses rely on a signatures-based methodology to detect threats by “comparing the discovered malicious patterns to the newly observed ones” (Chen 2018, p. 244). APTs, however, do not conform to this methodology as they exploit vulnerabilities to bypass these mainstream techniques (Chen, 2018). Due to their dynamism, there is an advocation for the incorporation of AI and ML to augment human-centric APT detection capabilities in the IoT especially as secured services in the cloud require “anomaly detection, diagnosis, and mitigation” (Trakadas 2019, p. 4) while an ML architecture can create correlation models to detect intrusion techniques “within each stage of the APT lifecycle” (Ghafir 2018, p. 351) for predictive analytics. This corresponds to the use of statistical modeling to analyze the complex, multi-phased nature of APTs incorporating the variables of duration and probability to evaluate each stage of an APT attack (Kumar, 2021), create a predictive framework for the propagation of malware worms (Zhou, 2021), and evaluate the likelihood of exploitation based on “chaining marginal and conditional probabilities to characterize the multiple attack paths” (Zimba 2020, p. 502) of advanced persistent threats. APT countermeasures blend behavioral characteristics with cyber defense paradigms since the behaviors of malicious actors and their unsuspecting victims influence the effectiveness of

implemented defense strategies. The best security protocols can be rendered ineffective if the user decides to "use their pet's name as their password, thus providing a simple path for an attacker to negate the strong security protocol" (Patterson 2019, p. 23).

Summary

The literature review explored the aspects of intrinsic identity uniqueness through the lens of the IoT and its data-centric nature that requires innovative approaches to cyber defense. Cyberspace itself "has unique peculiarities, made possible by its partial immateriality and expansive interconnectivity" (Medeiros and Goldoni 2020, p. 37). The complexity, fluidity, persistency, and boundary-less properties of the IoT require an evolution from traditional perimeter-based cybersecurity paradigms anchored in known intrusion signature detection and mitigation measures. Data is a strategic asset in the modern IoT as it is the foundational fabric for H2H, H2M, and M2M interactions and transactions. Commoditized data is a convergence of the physical and digital worlds whose interoperability has eased data sharing but demands enhanced accountability as the ubiquitous nature of the IoT is a continuous attack surface that is progressively multi-vectored and multi-layered. The adaptive heuristics of malicious actors have significantly increased the cost of cyber defense as data itself can either be exploited or become a weaponized platform. The open architecture of the IoT offers the malicious actor opportunities to maintain anonymity, conceal intent, and covertly recruit like-minded individuals through near-instantaneous social networking and digital collaboration. Identity-based cognitive machine symbiotic cybersecurity policies, coupled with distributed ledger technologies, support the transition of cyber defense methodologies from a network-centric, bastion approach to a data-centric, distributive one where humans and machines must verify their identities before engaging

in data transactions as a countermeasure for credentials tampering as malicious actors seek to masquerade as legitimate IoT users.

The necessities of digital identities verification become important as virtualization has separated the identities of applications and digital services from the identities of the physical servers hosting them thus impacting the areas of access control (both role-based and access-based), credentialing, authorizations, data management, privacy and digital rights management, and digital service deliveries. As the IoT enables the commoditization of data, a cognitive machine operating within this ubiquitous environment requires granular capabilities to assemble digital identities that conform with policies enforcing uniformity across heterogeneous platforms and attributes that "can be dynamic and…change with the membership of identity collection" (Pal 2018, p. 49). As modern societies continue their datafication, the methods that are implemented to verify "who" the user is in the digital environment becomes critical to prevent the malicious use of big data (Cheney-Lippold, 2017) as societies live "in a world where our reality is augmented by data" (Cheney-Lippold 2017, p. 265). As malicious actor exploits in the decentralized and distributed nature of the IoT can include the perpetuation of fake data, user impersonation to obtain access to big data, or compromise authenticated certificates (Li, 2020), policies strengthening the digital uniqueness of cognitive machines are important as machines are increasingly partners to human activities with their unique behaviors and cognitive abilities.

Though policies to standardize the attributes of digital identities are not a panacea to completely counteract the actions of malicious actors, they are critical for the creation of a modernized cyber defense model linking the strengths of governance, technological innovation, user behaviors, and business processes. Malicious actors can execute operations "to research a target, prepare it for penetration, dispatch an agent, and establish a presence that…affords access

to the desired information for exfiltration" (Riehle 2019, p. 192) where "the advent of digital storage, information can potentially be accessed remotely without the need for a physical presence inside a secured space" (Riehle 2019, p. 191). The adversarial threat is no longer a simple, faceless virus or other forms of malware. Instead, it is a skilled human(s) or cognitive machine(s) (or a malicious HMT) possessing deliberative intent and motivation who does not believe that it is either unethical or immoral to exploit digital technologies and cyberspace.

CHAPTER THREE: METHODS

Overview

The decentralized, distributed, and social nature of the IoT possesses native cybersecurity vulnerabilities as its public architecture makes data "accessible to various organizations and domains across the internet" (Khan 2020, p. 10). As IoT devices collect information about their owners, the availability of such data "creates a significant number of targeted attacks, both against the human user and functional objects" (Mustafaev 2020, p. 1). This study employed a quantitative, correlational archival data research design. For RQ1, the frequency of malicious software attacks was the dependent variable and diversity of intrusion techniques was the independent variable. For RQ2, the frequency of detection events was the dependent variable and diversity of intrusion techniques was the independent variable. The purpose of this study is to postulate a design framework for symbiotic cybersecurity policies incorporating cognitive machine individualism to enhance the implementation of human-machine teaming (HMT) in the preservation of IoT integrity. The descriptions of the research design provide the reader with the analytical context linking malicious software exploitations, intrusion techniques, and the frequency of detection events as a paradigm framing the symbiotic cybersecurity policy triad and the role of cognitive machine digital identities.

Role of the Researcher

The researcher is responsible for outlining the foundations of the study and answering its questions including designing the study, performing data collection and maintenance, and analyzing, interpreting, and reporting its findings. The researcher is a civilian contractor supporting the Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)) digital modernization initiatives and a 26-year veteran of the US Army Reserves

with operational deployment experience. The researcher is a Certified Enterprise Architect (CEA) with experience as a technical portfolio manager and project manager with a technical background in requirements and capabilities determination, network and infrastructure management, and emergent data-centric principles.

Design

A correlation archival data design was used for the study. Implied in this research is the identification of a potential correlation between the frequency of malicious software attacks and the diversity of intrusion techniques. Behaviorally, modern malicious actors conduct targeted exploitations based on a disciplined operational framework where those actions erode the IoT trust model. User interactions (and data access) within the IoT are based on a presumption that both the implementation of the system and "the operation of the protocol" (Vella 2020, p. 229) are secured. Assessing the correlation between the frequency of malicious software attacks and the diversity of intrusion techniques assists in the analysis and investigation of potential patterns associated with the variables. These potential patterns can help inform the prioritization of factors important to the creation of identity-based symbiotic cybersecurity policies and the significance of adopting the symbiotic cybersecurity policy triad.

Descriptions and Rationale for the Methods to be Employed

The proposed quantitative study incorporates a descriptive statistics procedure focusing on malicious software attacks and intrusion techniques to establish a distribution pattern baseline. A correlational coefficient bivariate analysis is utilized to measure the strength between two variables. A *Pearson r* correlational coefficient test is used if the data possesses a normal distribution or *Spearman's rho* if the data has a non-normal distribution. Determining correlational strength does not infer probabilistic trends but rather, it provides insight to visualize

patterns of malicious behavior in analyzing the feasibility of formulating identity-based cognitive machine symbiotic cybersecurity policies codifying machine digital distinctiveness and individualism.

D'Agostino (2019) detailed the CyberSAR project that focused on the adoption of intelligence-enabled security heuristics based on epidemiological best practices (D'Agostino, 2019). The approach utilizes a time-based comparison of domain name server (DNS) traffic "to measure the volume of detected anomalies associated with known or unknown cyber threat behaviors in the treatment and control groups" (D'Agostino 2019, p. 23). This methodological approach treats the digital environment as an ecosystem of interrelated (and interconnected) systems (D'Agostino, 2019). Chen et al (2020) elaborate on this approach as the researchers propose a detection and analysis model based on gene sequencing of software (Chen, 2020) to compare malicious intrusion signatures to a software gene pool using "a genetic model based on the contents of file node and action node" (Chen 2020, p. 5). The model is comprised of the detection mechanism, the malware environment, the system file of interest, the system object that the malware operates in, and the description of the intrusion (Chen, 2020). Adopting public health methodologies for cyber defense is an innovative application of behavior-based pattern analysis analogous to the medical profession testing, diagnosing, and treating infectious diseases based on known symptomatic signatures. These innovative paradigms recognize the adaptive heuristics of malicious threats in the IoT as the traditional bastion approach of defending at network boundaries is insufficient since data itself is a weaponized platform for exploitation. Innovative defense requires the ability to overcome the uncertainties of attack vectors and malicious actor strategies (Xie, 2021) that is feasible if counterthreat mechanics incorporate the behaviors and motivations of malicious actors to enhance insights into the "where", "who", and

"why" these adversaries will target specific users and systems to fulfill their strategic initiatives. Bhattacharjee (2018) postulates that the convergence of the physical and cyber worlds translates into "proactive detection and remediation, digitally tracking the supply chain…and many similar use cases" (Bhattacharjee 2018, p. 11) as the ubiquitous IoT environment creates a persistent attack surface. As data is the core of the IoT, identity-based protection and preservation schemas apply to all users "to guarantee the delivery of trustworthy decisions" (Janssen 2020, p. 1). Information Age interoperability and integration have eased data collection and sharing but demand enhanced accountability to ensure that legitimate users are granted access to IoT resources particularly if the user is a cognitive machine.

Conceptual and Operational Definition of the Variables Explained

Empirical statements are a critical framework for defining the conceptual and operational contexts of the variables within this research and are outlined below:

- Digital exploitations are correlated to the utilization of malicious software.
- Digital exploitations are correlated to the organizational, doctrinal, or ideological behaviors of advanced persistent threats.

ES1 stipulates that a positive correlation exists between malicious software and the techniques malicious actors utilize against targeted systems and users. The correlational strength between malicious software attacks and intrusion techniques can inform the development of predictive modeling and threat analysis to operationalize countermeasures based on the compilation and cataloging of intrusion signatures. The ability to assess the effectiveness of identity-based cognitive machine symbiotic cybersecurity policies is dependent on the ability to aggregate and link patterns of cyber intrusions that parallel the public health approach of pattern analysis and symptomatic associations enabling providers to isolate threat indicators for specific diseases and recommend the proper treatments. Incorporating pattern analysis into an

interdisciplinary cybersecurity policy framework leverages identifiable intrusion signatures as a behavioral component that can be coupled with the creation of baseline cryptographic schemas to mitigate vulnerabilities associated with identity authentication and access management.

ES2 stipulates that a positive correlation exists between digital exploitations and the organizational, doctrinal, or ideological behaviors of malicious actors. Ahmad et al (2019) note that advanced persistent threats represent organized entities that "apply resources in deliberate ways to attack…assets" (Ahmad 2019, p. 403). Malicious actors do not operate in isolation and their goals are "human-driven, strategically motivated operations" (Ahmad 2019, p. 408) where intrusions are tied to a more expansive set of strategic objectives. Comprehending these goals shapes an understanding of their behavioral aspects and can lead to the innovative application of AI and ML capabilities to increase the integrity of cognitive machine digital identities as a mitigation factor for attempts to spoof (or forge) digital credentials as part of a malicious threat reconnaissance operation. DeVore and Lee (2017) state that the customized characteristics of advanced persistent threats mean that developers need access to technical intelligence on the organizations and systems targeted for exploitation (DeVore, 2017). To gain this kind of technical intelligence, a behavioral map should be constructed as part of a root cause analysis linking malicious actor activities to underlying influences behind those activities. Effective cyber threat management, mitigation, and remediation require insight into the behavioral motivations of malicious actors as comprehending those influences augments predictive modeling and threat analysis to shape proactive cyber defense approaches. Safeguarding its interconnected (and interdependent) data-driven digital infrastructure requires recognizing that the cyber threat is a method of power projection that seeks to take advantage of the digital terrain to achieve operational and strategic dominance. The IoT requires vigilance different from

traditional cybersecurity principles; enabling secure digital identities for cognitive machines could yield counter-exploitation tools where the machine can self-propagate trust across shared nodes. Perpetuating trust is the critical factor in countering behavior-based malicious cyber activities as the threat consistently seeks to exploit trust within the IoT as a method of gaining access to the voluminous libraries of transferred and curated data.

Description of the proposed means of investigation

To conduct a quantitative exploration into identity-based cognitive machine symbiotic cybersecurity policy design factors, the research design proposes a data collection framework utilizing the publicly accessible cyber incident data repositories listed below:

- MITRE Att&ck (www.attack.mitre.org)
- MITRE Cyber Analytics (www.car.mitre.org)
- MITRE Common Attack Pattern Enumeration and Classification (CAPEC) (www.capec.mitre.org/index.html)
- Council on Foreign Relations Cyber Operations Tracker (www.cfr.org)
- Center for Strategic and International Studies Strategic Technologies Program (https://www.csis.org/programs/strategic-technologies-program)
- Alien Vault Open Threat Exchange (https://otx.alienvault.com/)
- Cisco Talos Intelligence Group (www.talosintelligence.com)

The cyber data repositories provide open-source knowledge on documented intrusion tactics, techniques, malicious actor groups, targeting behaviors and patterns, and mitigation strategies. This open-source knowledge permits the establishment of an initial pattern of life baseline connecting malicious actor behavioral commonalities with targeting activities, cyber intrusion tactics and techniques used, and degrees of operational sophistication across a diverse set of attributes. Chen et al (2018) state that traditional firewalls and anti-viruses rely on a signatures-based methodology to detect threats by “comparing the discovered malicious patterns to the newly observed ones” (Chen 2018, p. 244). Malicious actors in the IoT, however, do not conform to this methodology as they exploit vulnerabilities to bypass mainstream cybersecurity

techniques (Chen, 2018). Analyzing the feasibility of implementing an identity-based symbiotic cybersecurity architecture incorporating cognitive machine individualism requires a base understanding of malicious actor behaviors within the IoT. Identity-based cognitive machine symbiotic cybersecurity is an evolution from the traditional network-centric, bastion approach to a data-centric, distributive one as the persistent connectivity of the IoT enables rapid access and exchange of digital resources within the context of social interrelationships. The ingested datasets are partially comprised of Microsoft (MS) Excel-based output files containing cyber-attack matrices listing known malicious actor groups, tactics, techniques, and utilized software malware obtained from the MITRE Att&ck data repository (www.attack.mitre.org/versions/v12.1) to provide the descriptive statistics between intrusion tactics and their associated techniques. Additional output files are comprised of an analytical coverage comparison cross-walk obtained from the MITRE Cyber Analytics Repository (www.car.mitre.org) that serves as a cross-referential datapoint between detection schemas and intrusion techniques, a cyber intrusion risk assessment matrix obtained from the MITRE Common Attack Pattern Enumeration and Classification (CAPEC) (www.capec.mitre.org/index.html) providing an organized categorization of attack patterns and a cross-reference between the CAPEC and the MITRE Att&ck data repositories.

Data Source Descriptions

Tables 1 and 2 are the open-source cyber data repositories contained in this section. These data sources are organized into two categories defined as:

- Primary sources supporting the bivariate analysis.
- Primary sources providing amplifying analytical data to support the feasibility assessment of cognitive machine SSI as a component of cohesive cybersecurity policies.

Table 1.

Primary Sources for Bivariate Analysis

Data Source	Description
MITRE Att&ck (www.attack.mitre.org)	A data repository of adversarial tactics and techniques based on real-world observations. The repository is utilized for the development of threat models and methodologies in cybersecurity communities across the public and private sectors. It contains documented information on 122 known APT groups whose activities span 215 cyber intrusion techniques consolidated into 14 tactical categories. APT groups are documented with attributed sponsors, cyber intrusion techniques used, software used to conduct the cyber exploitations, and associations with other known APT groups (Att&ck, n.d.)
MITRE Cyber Analytics (www.car.mitre.org)	An analytical knowledge base developed from the MITRE Att&ck model that describes an observable behavior associated with an APT intrusion tactic or technique to facilitate predictive modeling. The repository contains 97 separate analytics mapped to 83 intrusion techniques or sub-techniques from the MITRE Att&ck repository.
MITRE Common Attack Pattern Enumeration and Classification (CAPEC) (www.capec.mitre.org/index.html)	A catalog of common attributes and approaches associated with adversarial attacks to create patterns of behavior; these patterns contain information on adversarial exploitation behaviors to include techniques adversaries use to adapt to countermeasures. The MITRE CAPEC was developed as part of the US Department of Homeland Security Software Assurance strategic initiative as a standardized mechanism for identifying, collecting, and sharing APT attack patterns across the cyber communities. The catalog contains 541 documented attack patterns that are further cross-referenced to the Web Application Security Consortium (WASC) Threat Classification taxonomy, the MITRE Att&ck tactics and techniques repository,

	and the Open Web Application Security Project (OWASP) taxonomy to construct a comprehensive attack schema and classification taxa
Council on Foreign Relations Cyber Operations Tracker (www.cfr.org)	A catalog of state-sponsored cyber threat actors was created to identify instances where political states utilize cyber proxies to pursue specific foreign policy goals and interests (CFR, n.d.). The catalog provides a timeline of significant cyber incidents from 2005 to the present and an interactive map listing incidents based on nation-state sponsors.

Table 2

Primary Sources of Amplifying Data

Data Source	Description
Center for Strategic and International Studies Strategic Technologies Program (https://www.csis.org/programs/strategic-technologies-program)	A project designed to provide data-driven analysis in the fields of cybersecurity, privacy and surveillance, technology and innovation, and internet governance (CSIS, n.d.). The STP maintains a series of project knowledge bases including the Significant Cyber Incidents Tracker which is a formatted event timeline starting in 2006 and focusing on cyber-attacks across governmental agencies, defense, technology companies, and economic crimes where the loss is greater than US$1 million (CSIS, n.d.). The tracker is organized in a month-year format with key data point summaries of the documented cyber incidences
Alien Vault Open Threat Exchange (https://otx.alienvault.com/)	A members-only HTML-based knowledge portal maintained through Alien Labs provides real-time and real-world documentation of malicious cyber activities where analysts and cybersecurity professionals broadcast a comprehensive summation of threats to create threat intelligence profiles informing cybersecurity community members (OTX, n.d.). The knowledge portal maintains over 445 sub-groups spanning a multitude of different cybersecurity interest fields (there is a sub-

	group specifically for APTs), has 58 million documented threat indicators, 24,000 malware families, and 346 known adversaries impacting 19 different industries (OTX, n.d.). Furthermore, the knowledge portal contains an interactive malware cluster map to view documented incidents based on the malware family. The knowledge portal leverages the disciplined processes of the Intelligence Community to overlay a behavioral context on the technical aspects of APT cyber exploitation and malicious activities.
Cisco Talos Intelligence Group (www.talosintelligence.com)	A commercial threat intelligence team comprised of researchers, analysts, and engineers (Talos, n.d.) focused on producing actionable intelligence through the collection of threat telemetry data spanning networks, endpoint devices, cloud and virtualized environments, and traffic monitoring of the internet (Talos, n.d.) on behalf of Cisco customers. The Talos Intelligence Group maintains a comprehensive HTML-based knowledge base containing a downloadable open-source software repository for malware detection, network scanning, encryption, intrusion detection and analysis, and dynamic data management; vulnerability assessment reports focused on zero-day and disclosed vulnerabilities; a series of correlational databases compiling real-time security intelligence data on network traffic by IP address and domain; and a library of documented cyber-attack incidents and case studies

Research Question(s)

The research questions below were investigated:

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

The study acknowledges that data is the core of the IoT and that guarding it is the "highest priority area for investment in cybersecurity" (Steadman 2021, p. 1) as the libraries of stored and curated data within the IoT are continuously vulnerable to the dynamics of human and malicious machine behavior. The data-centric nature of the IoT prioritizes the necessities of human-cognitive machine symbiosis leveraging the scalable capabilities of cognitive machines (that learn with continued ingest of data) to assume shared responsibilities for preserving IoT integrity.

Hypothesis(es)

The null hypotheses for this study are:

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

- $H_0$1: There is no statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.
- H_a1: There is a statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

- $H_0$2: There is no statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.
- H_a2: There is a statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.

The persistency of stored data in the IoT is a constant area of vulnerability requiring the implementation of increasingly complex multi-factor authentication protocols to verify legitimate users requesting services and data, secure the data-in-transit, and authenticate the infrastructure components handling the data. Designing a trusted digital ecosystem to mitigate the probability of malicious software exploitations requires cyber defenders to develop

innovative methods across virtual ecosystems. Cognitive machines alter the paradigms of trust in their ability to imitate human behavior through data transference in the IoT. The interaction through data creates a newfound complex web of social relationships between humans and machines comprised of friendship, ownership, and community. Identity-based cognitive machine symbiotic cybersecurity policies focus on governance and business processes to ensure verifiable credentials are exchanged in a P2P environment based on trust concepts anchored in ethical behaviors to safeguard the open data-sharing standards of the IoT.

Dataset

The MITRE Att&ck dataset was obtained through an open-source download from MITRE with version 12.1 containing 14 tactics, 193 techniques, 401 sub-techniques, 134 documented malicious actor groups, 14 campaigns, and 718 documented malicious software used for intrusions and exploitations. Table 3 is the tactics parameter and the associated number of techniques.

Table 3

MITRE Att&ck Tactics and Number of Associated Techniques

Tactic	Number of associated Techniques
Reconnaissance	**10**
Resource Development	**7**
Initial Access	**9**
Execution	**13**
Persistence	**19**
Privilege Escalation	**13**
Defense Evasion	**42**
Credential Access	**17**
Discovery	**30**
Lateral Movement	**9**
Collection	**17**
Command and Control	**16**
Exfiltration	**9**
Impact	**13**

The MITRE Cyber Analytic Repository (CAR) dataset was obtained through an open-source download from MITRE. The dataset is an analytical crosswalk between the CAR, Sigma, Elastic Detection, and Splunk Security Content threat detection environments. The dataset contains 541 individual threat entries with a total of 9,986 detection incidents organized based on 187 different intrusion techniques. The MITRE Common Attack Pattern Enumeration and Classification (CAPEC) dataset was obtained through an open-source download from MITRE. The dataset contains a catalog of common attack patterns to enable a shared understanding of how malicious actors exploit weaknesses in the cyber domain. The dataset has 546 individual pattern entries with parameters of description, likelihood, severity, relations, execution flow, prerequisites, skills required, resources required, indicators, consequences, mitigations, related weaknesses, and taxonomy mapping.

The IoT is an interdependent ecosystem of technological applications, digital services, and behavior-based (both attributional and reputational) access control. As the sophisticated and organized exploits of modern malicious actors continue, correlational analysis becomes critical in identifying patterns to help human-cognitive machine cyber defenders to "see the full scope of the incidents" (Rajivan and Cooke 2018, p. 627). Rajivan and Cooke (2018) used a lab experiment with two specific simulated cyber incidents (and associated synthetic data) where thirty teams of 3 assigned ownership of subnetworks to test their postulation that "analysts would…often communicate incidents that are conspicuous" (Rajivan 2018, p. 628) to gain validation from others. Manual communication is suboptimal as it tends to focus on the isolated observations of each team and hampers the ability to correlate across teams to establish

associations that would lead to the discovery of the full extent of the cyber-attack (Rajivan, 2018).

Xu et al (2018) investigated the use of stochastic processes to describe data breach incidences including size and arrival frequency as the 7,730 documented data breaches between 2005 and 2017 accounted for "9,919,228,821 breached records" (Xu et al 2018, p. 2856). The dataset used for the study contained "600 hacking breach incidents in the United States between January 1st, 2005 and April 7th, 2017" (Xu 2018, p. 2858) spanning 7 different industries. The study used an autoregressive conditional mean point process (Xu, 2018) and an ARMA-GRACH time series model to analyze the evolution of the breach size and volatility (Xu, 2018). The statistical modeling was developed for predictive analytics based on temporal correlations and recognizing the dependency between "incidents inter-arrival times and the breach sizes" (Xu 2018, p. 2869).

Song et al (2021) quantitatively analyzed eight national cybersecurity strategies using natural language processing for data mining of unstructured text data. Their study used topic modeling as a "statistical technique…to discover hidden structures from collections of documents" (Song et al 2021, p. 62). The dataset is comprised of the national cybersecurity strategies of the United States, United Kingdom, Japan, and the European Union with 1,287 different words used for the actual topic modeling analysis (Song, 2021). Aggregating constituent words, the study identified fifteen agendas common to the collected national cybersecurity strategies organized into the four sectors of Infra Stability, Protection and Response Capability, Industry and Technology, and International Cooperation (Song, 2021). The quantitative analysis explored the differences in approaches between the national cybersecurity strategies based on distribution factors of agendas and sectors across the dataset.

The analysis also explored changes in strategies over time as the collected documents span the periods between 2003 and 2020 (Song, 2021). The correlation between the distribution of agendas and the "perceived cyber threat environment" (Song 2021, p. 69) influences the macro-level cybersecurity approaches for recognized international leaders in technological adoption. This correlation is important as cybersecurity policy is multi-dimensional and encompasses "multi-lateral cooperation efforts across society, government, science, technology, industry, and academia" (Song 2021, p. 69).

Cheong et al (2021) examined how a public firm's "disclosure behaviors regarding cybersecurity risks are different from other firms when the firm experienced a cybersecurity incident or received an adverse SOX 404 opinion" (Cheong et al 2021, p. 180). The SOX 404 refers to section 404 of the Sarbanes-Oxley Act of 2002 where auditors must attest to the internal controls for financial reporting and report internal control weaknesses (Cheong et al, 2021). The dataset is comprised of 25,179 cybersecurity risk disclosures from 4,918 companies between 2006 and 2017 (Cheong, 2021). The research questions center on whether the context of cybersecurity risk disclosures of firms differ for those who experience a cyber breach or receive an adverse SOX 404 opinion from those who do not (Cheong, 2021). The study used a Latent Dirichlet Allocation (LDA) topic model to conduct a textual data analysis based on the identification of "topics related to cybersecurity" (Cheong 2021, p. 183). An exploratory factor analysis was used to classify 30 topics into nine factors: incident control and risk mitigation, operational risk, customer-related, contract-related, business continuity, payment system, network security, third-party software providers, and assurance (Cheong, 2021). The study developed a "regression model on risk factors to examine the contextual differences" (Cheong 2021, p. 185) where it was discovered that breached firms "disclosed less information about

incident control and risk mitigation and business continuity" (Cheong 2021, p. 188) while focusing more on third-party software providers (Cheong, 2021). It was also discovered that firms who received an adverse SOX 404 opinion tended to "disclose more information about operational risk" (Cheong 2021, p. 188). Organizational behavior in the aftermath of an adverse cyber event is important to understand as who an organization believes is responsible for the cyber vulnerabilities shapes their remediation strategies.

Variables

Dependent Variable: *frequency of malicious software attacks*

MITRE defines malicious software as "custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in Att&ck" (MITRE, n.d.). Threat actors execute malicious software exploitations through a multitude of techniques including duplicating network traffic; using alternative protocols such as FTP, SMTP, HTTP/S, DNS, or SMB; using command and control channels; or infiltrating data repositories. Malicious software exploitations are measured in a post-data normalization analysis of the MITRE Att&ck dataset based on the unique identification code MITRE assigns to documented malicious software. Within the dataset, malicious software entries are mapped to intrusion techniques, known threat actor groups, and recommended mitigation techniques. The mapping provides expanded traceability to establish patterns of life for the purposes of analyzing the relational dimensions of malicious operations. Further measurements are obtained through descriptive statistics of the Att&ck dataset to determine if specific malicious software has greater prevalence and if there are unique characteristics associated with them. The additional measurements enable analysis into the nature of malicious software particularly those that possess their own form of machine cognition. Appendix B contains the list of documented

malicious software within the MITRE dataset and their unique identifiers.

Independent Variable: *diversity of intrusion techniques*

Intrusion tactics represent the "adversary's tactical goal" (MITRE, n.d.) spanning a multitude of techniques designed for multi-variate exploitation. These techniques are how adversaries achieve their "tactical goal by performing an action" (MITRE, n.d.). In the context of digital identities, Haber and Rolls (2019) state that threat actors use methods "to compromise an identity and impersonate it for their malicious intent…the goal of the threat actor is to own you at the highest level possible and impersonate you as far down the account chain as possible" (Haber 2019, p. 107). Intrusion techniques are measured in a post-data normalization analysis of the MITRE Att&ck, CAR, and CAPEC datasets based on the unique identification code MITRE assigns them. Much like the framework for the dependent variable, these techniques are mapped to malicious software, intrusion tactics, and known threat actor groups to provide expanded traceability for patterns of life analysis. Table 4 below lists the intrusion tactics within the MITRE Att&ck dataset and their unique identifiers to provide a baseline traceability between intrusion techniques and tactics.

Table 4

MITRE Att&ck Intrusion Tactics and their Unique Identifiers

Tactic	Unique Identifier
Initial Access	**TA0001**
Execution	**TA0002**
Persistence	**TA0003**
Privilege Escalation	**TA0004**
Defense Evasion	**TA0005**
Credential Access	**TA0006**
Discovery	**TA0007**
Lateral Movement	**TA0008**
Collection	**TA0009**
Exfiltration	**TA0010**
Command and Control	**TA0011**

Impact	TA0040
Resource Development	TA0042
Reconnaissance	TA0043

Conceptualization and Measurement

Mousavi et al (2021) describe the six characteristics of objects in the IoT as existence, self-identity, communication, interaction, dynamicity, and environmental awareness (Mousavi et al, 2021). The IoT permits users "to observe their status, implement remote control and management, perform infrastructural configuration, and search devices" (Mousavi et al 2021, p. 1517) through sensor technologies, cognitive machines, and digital services. Identity authentication is critical for the mitigation of disguised attacks from malicious actors, especially as the successful exploitation of a smart object means "its sensing information is seized by the attacker for spying purposes in the enterprise" (Mousavi 2021, p. 1516). The dynamic state of the IoT (with its data persistency) has revealed a wide range of security vulnerabilities "from authentication to trust management" (Mousavi 2021, p. 1551) due to its data persistency. Data continuously flows between digital environments, devices, users, and services but more importantly, stored and curated data continues to live in the virtual space and remains accessible to both legitimate users and malicious actors. Yusif and Hafeez-Baig (2021) state that dynamic cybersecurity strategies are not viewed from a vulnerability perspective (Yusif and Hafeez-Baig, 2021) but rather "from the perspectives of resiliency and active cyber defense" (Yusif and Hafeez-Baig 2021, p. 499), particularly as data breaches are on the rise (Yusif, 2021). In 2015 alone, the Interstate Technology and Regulatory Council "identified 781 breaches" (Yusif 2021, p. 494) that exposed 169 million records (Yusif, 2021) amounting to a 63.8% increase in breaches over a six-year timeframe and a staggering 768% increase over a decade (Yusif, 2021).

Data persistency in the IoT requires identity-based symbiotic cybersecurity policies to focus on extending behavioral concepts of social trust into the digital space. The Buecher-Tavani model of digital trust defines these trust relations as trust between human agents, trust between human agents and AA (artificial agents), and trust between AAs (Buecher, 2020). In a revision of the Buecher-Tavani model, Buecher (2020) examines the concept of self-trust incorporating the idea that "trust is incompatible with a reductive view of self and compatible with the existence of a substantial self" (Buecher 2020, p. 1). The model has five conditions based on the behavioral relationship and expectations between two subjects (known as "A" and "B"). Those conditions are that A possesses a normative expectation that B will perform certain actions (that are not necessarily pre-defined), that B is responsible for the normative expectation of A, that A has a disposition to normatively expect that B will perform actions responsibly, that A's normative expectation of B's actions can be mistaken, and that A develops a disposition to trust B (Buecher, 2020). H2M and M2M interactions in the IoT are the data exchange expressions of these agent relationships as humans interact with cognitive machines as if the machines have a form of a substantial self. It can be argued that a sense of self cannot be programmatically (or computationally) enabled in machines, yet IoT interactions are based on the paradigms of human social communication. The cognitive machine (as the AA) performs actions in a model of reciprocity where the machine can make inferences and decisions without consulting a human; think of the smart vehicle technologies that can drive (and park) the car or engage safety features without the human in the loop. The smart vehicle continuously interprets collected data and dynamically adjusts to its environment rather than solely reacting based on programming scripts. The cognitive machine (as an AA in the IoT) is a participating actor

whose digital persona mimics common human behavioral traits including the ability to adapt based on changes in social or physical environments.

Procedures

Phase One (Open-Source Data Collection)

Phase one is data collection from publicly accessible cyber incident data repositories.

- MITRE Att&ck (www.attack.mitre.org)
- MITRE Cyber Analytics (www.car.mitre.org)
- MITRE Common Attack Pattern Enumeration and Classification (CAPEC) (www.capec.mitre.org/index.html)

The cyber incident data repositories provide open-source knowledge on malicious actor groups, exploitation tactics and techniques, targeting behaviors and patterns, and mitigation strategies. This open-source knowledge permits the establishment of an initial pattern of life baseline for assessing the correlational relationship between identity-based exploitation techniques and malicious actor activities using the exploitation tactic.

Phase Two (Data Cleansing and Normalization)

Data cleansing improves data quality through the elimination of data inconsistencies and errors. These inconsistencies and errors can include mislabeled columns and rows, data entry errors, incorrect data types, and null fields. The process of cleansing prepares the datasets for normalization which organizes the data into a common structure to establish consistencies across records and data fields. Each dataset has achieved the first normal form (1NF) which requires that each cell in the data table is unique and that the records are distinct. To achieve the second normal form (2NF) for the MITRE Att&ck dataset, a data taxonomy is built with unique intrusion identifier values assigned to each intrusion tactic. Table 5 contains the unique intrusion identifier values.

Table 5

Unique Intrusion Identifier Values for MITRE Att&ck 2NF

Intrusion Tactic	Identifier Value
Reconnaissance	**1**
Resource Development	**2**
Initial Access	**3**
Execution	**4**
Persistence	**5**
Privilege Escalation	**6**
Defense Evasion	**7**
Credential Access	**8**
Discovery	**9**
Lateral Movement	**10**
Collection	**11**
Command and Control	**12**
Exfiltration	**13**
Impact	**14**

To achieve 2NF in the CAPEC dataset, the "high/medium/low" ratings for likelihood and severity factors convert into numeric values on a scale of 1-5 according to Table 6.

Table 6

Unique Identifier Values for Likelihood and Severity Factors

Ratings	Identifier Value
Very Low	**1**
Low	**2**
Medium	**3**
High	**4**
Very High	**5**

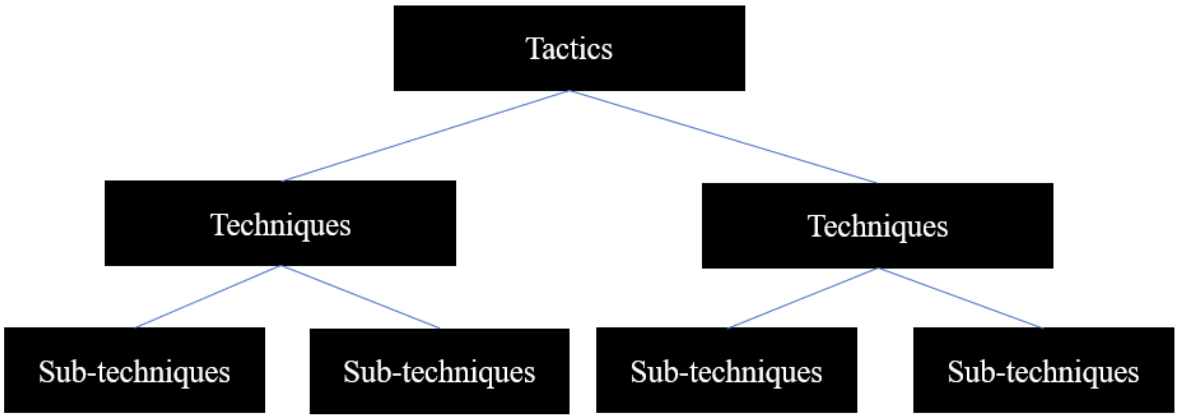
Zahid et al (2020) present a formula for calculating risk that is expressed as *risk = likelihood of occurrence x severity of risk* (Zahid et al, 2020). Conversion to numeric values permits the creation of a scatterplot to document the aggregated risk at the parent attack pattern level.

Terminology Hierarchy

Figure 4 is the hierarchy of terms representing the parent-child and one-to-many relationship between the intrusion terminology within the datasets.

Figure 4

Intrusion Terminology Hierarchy



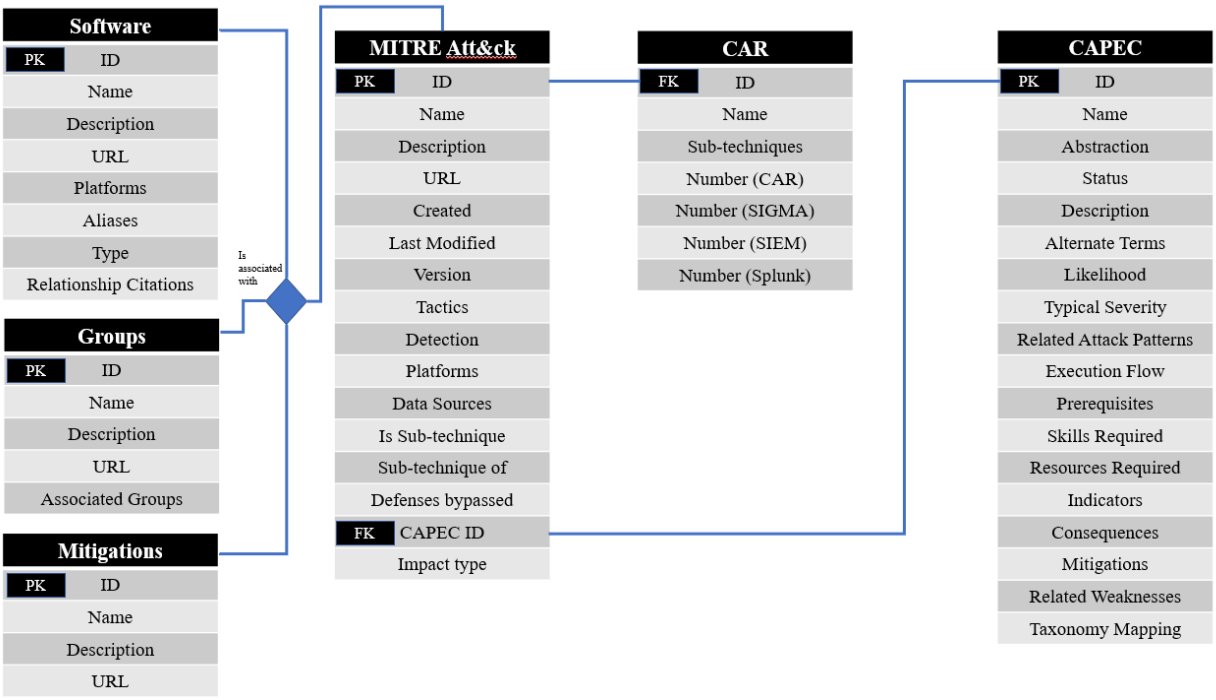
Note. The image is a representation of the relational hierarchy used within the MITRE Att&ck repository (www.attack.mitre.org/)

Entity Relationship Diagram

Figure 5 is the entity relationship diagram (ERD) illustrating the data fields associated with each dataset, the primary key (PK), the foreign key (FK), and the linkages between the datasets.

Figure 5

MITRE Data Fields Entity Relationship Diagram (ERD)



Note. The image is a representation of the data field relationships between the datasets collected from the MITRE Att&ck repository (www.attack.mitre.org/), the MITRE Cyber Analytics repository (www.car.mitre.org), and the MITRE CAPEC repository (www.capec.mitre.org/index.html)

Phase Three (Post-normalization)

The post-normalization analysis explores patterns in the data based on the aggregated attributes of all three datasets. The pattern analysis focuses on capability tracing at the technical

level to establish relationships between techniques, malicious groups, software, mitigations, the likelihood and severity factors, and detected incidents. The pattern analysis permits clustering based on themes and factors to enrich the statistical analysis.

Data Analysis

A *Pearson r* correlation coefficient is a ratio where "the scale of variables becomes a non-issue" (Denis 2021, p. 74) as the bivariate relationship is dimensionless (Denis, 2021). A *Spearman's rho* correlation coefficient "reflects the relationship between two variables, but it is not restricted to that relationship necessarily being linear in form" (Denis 2021, p. 76). This study adopts a bivariate analysis with a *Pearson r* to evaluate both RQ1 and RQ2 if the data possess a normal distribution or a *Spearman's rho* if the distribution is non-normal. The hypotheses for RQ1 and RQ2 are expressed below.

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

- $H_0$1: There is no statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.
- H_a1: There is a statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

- $H_0$2: There is no statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.
- H_a2: There is a statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.

It is assumed that malicious actors are organized entities that execute intrusions and exploitations based on specific operational or behavioral paradigms. Determining the frequency

of malicious software attacks and the diversity of intrusion techniques is a determinant for assessing the magnitude of the threat.

Bivariate Analysis with Risk Scatterplot

For RQ1, the statistical correlation is paired with the CAPEC risk scatterplot to connect prevalence with the scope of the risk to provide a more holistic view of the nature of the malicious software threat. As modern malicious actors have their utility functions "and seek to maximize the effectiveness" (Insua et al 2019, p. 20) of their attacks, malicious software exploitation threat mitigation must combine behavioral probability (through pattern analysis) with a governance structure focusing on securing the user and their data rather than simply the network being used. The scatterplot augments the bivariate analysis through a visual depiction where probability of intrusions is compared to severity values. Those techniques assessed as "high" or "very high" in both probability and severity are analyzed to determine their associated intrusion mechanisms. Associating the mechanisms to the categorical risk amplifies the fundamental characteristics of each pattern of attack to aid in visualizing the scope of the threat.

Bivariate Analysis with Clustering

For RQ2, the statistical correlation is paired with a hierarchical cluster to organize the CAR data into an attribute-value distribution classification tree (Aggarwal and Reddy, 2018). The hierarchical cluster utilizes nodal relationships to organize data through "logical rather than probabilistic descriptions" (Aggrawal and Reddy 2018, p. 288). Hierarchical clustering enables the decomposition of the CAR data into a classification tree to demonstrate nodal relationships between intrusion tactics, detection schemas, exploited machine languages, and frequency of detections. Clustering is a visualization of associations to draw inferences to inform cyber public policy designs as cluster analysis enables traceability across multiple variables to determine

critical vulnerability characteristics or dependencies even if the RQ2 null hypothesis is true. For example, if a post-clustering analysis determines that a specific machine language is vulnerable to malicious intrusions, a traceability assessment can be initiated to determine the underlying causal determinators. Such an assessment informs policy design, specifically in the crafting of exploitation mitigation strategies based on traced technical vulnerabilities.

CHAPTER FOUR: FINDINGS

Overview

The IoT enables rapid data and information transfer but increases the probability of malicious cyber activity as the digital landscape provides the adversarial threat with a multitude of exploitation vectors. This study defined the variables for statistical testing based on known cyber intrusion tactics and techniques, patterns of attacks, and detection events; the description for the dependent and independent variables is outlined in Chapter 3. The research focused specifically on frequency of malicious software attacks, the diversity of intrusion techniques, and the frequency of detection events. The primary data sources are from the MITRE Corporation containing information on intrusion tactics and techniques, detection mechanisms, operating systems affected, machine languages affected, defenses bypassed, and recommended mitigations, among others. The study is framed within the research questions and hypotheses below.

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

- $H_0$1: There is no statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.
- H_a1: There is a statistically significant relationship between the frequency of malicious software attacks and the diversity of intrusion techniques.

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

- $H_0$2: There is no statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.
- H_a2: There is a statistically significant relationship between the frequency of detection events and the diversity of intrusion techniques.

Descriptive Statistics

The first set of descriptive statistics are from the MITRE Att&ck dataset (N = 10306) used for RQ1. The study used the IBM Statistical Product and Service Solutions (SPSS) software suite to generate descriptive statistics tables and figures. Reference appendix C for the full list of the individual total and % of total statistics for the MITRE Att&ck malicious software categorizations. Table 7 below contains the N statistics for the Att&ck dataset.

Table 7

Descriptive Statistics for Intrusion Tactics

Descriptive Statistics – Intrusion Tactics		
		Tactics
N	**Valid**	**10306**
	Missing	**0**

Table 8 below contains the individual total and % of total statistics based on the MITRE Att&ck malicious software categorizations.

Table 8

Malicious Software Categorization Frequency Analysis

Malicious Software Type					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**Tools**	**873**	**8.5**	**8.5**	**8.5**
	Malware	**9433**	**91.5**	**91.5**	**100.0**
	Total	**10306**	**100.0**	**100.0**	

Table 9 below contains the individual total and % of total statistics based on the MITRE Att&ck intrusion tactics categorizations.

Table 9

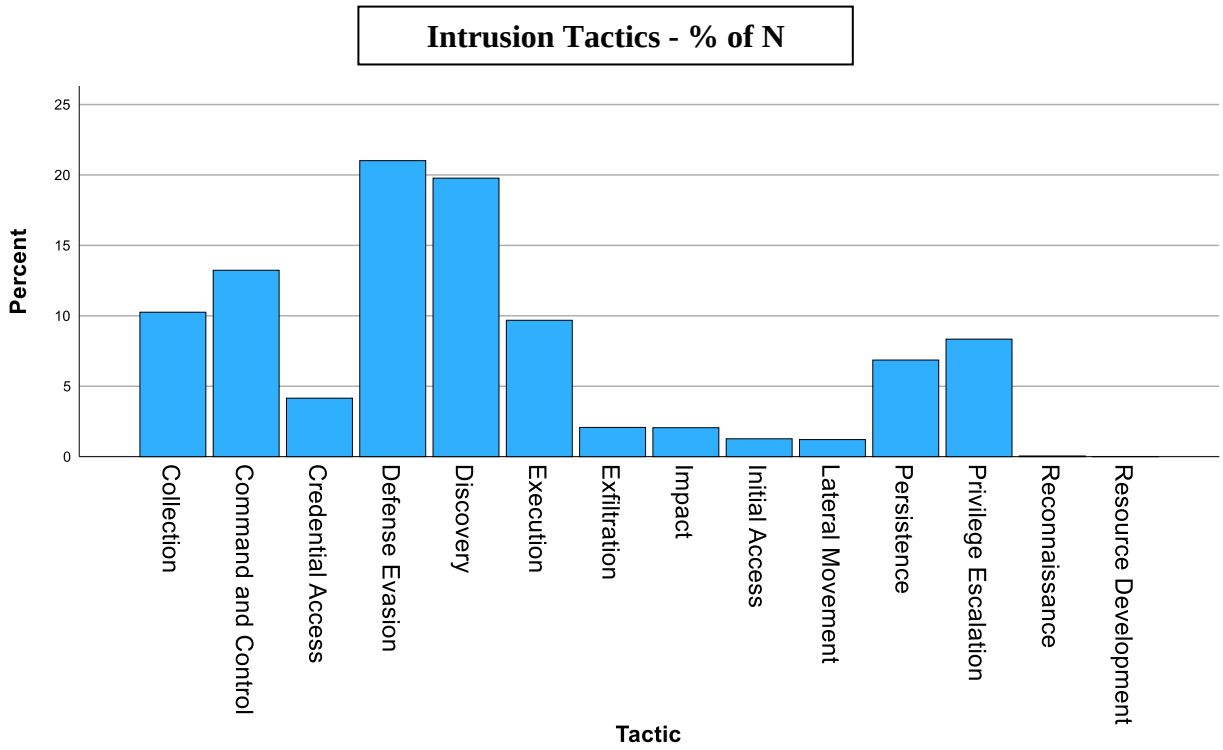
Intrusion Tactics Frequency Analysis

Tactic					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Collection	1057	10.3	10.3	10.3
	Command and Control	1364	13.2	13.2	23.5
	Credential Access	428	4.2	4.2	27.6
	Defense Evasion	2166	21.0	21.0	48.7
	Discovery	2038	19.8	19.8	68.4
	Execution	998	9.7	9.7	78.1
	Exfiltration	214	2.1	2.1	80.2
	Impact	212	2.1	2.1	82.3
	Initial Access	131	1.3	1.3	83.5
	Lateral Movement	125	1.2	1.2	84.7
	Persistence	707	6.9	6.9	91.6
	Privilege Escalation	860	8.3	8.3	99.9
	Reconnaissance	5	.0	.0	100.0
	Resource Development	1	.0	.0	100.0
	Total	10306	100.0	100.0	

Figure 6 below is a graphical representation of Table 8 containing the individual total and % of total statistics organized based on the MITRE Att&ck intrusion tactic categorizations.

Figure 6

Bar Chart Intrusion Tactics as % of N



The second set of descriptive statistics are from the MITRE Cyber Analytics Repository (CAR) dataset (N = 588) used for RQ2. Reference appendix B for the full list of the individual total and % of total statistics of the MITRE CAR intrusion technique categorizations. Table 10 below contains the N statistics for the CAR dataset.

Table 10

Descriptive Statistics of CAR Detection Mechanisms

Descriptive Statistics – Detection Mechanisms		
		Techniques
N	**Valid**	**588**
	Missing	**0**

Figure 7 below is a graphical representation of appendix B containing the individual total and % of total statistics organized based on the MITRE CAR intrusion techniques categorizations.

Figure 7

Bar Chart of CAR Intrusion Techniques as % of N

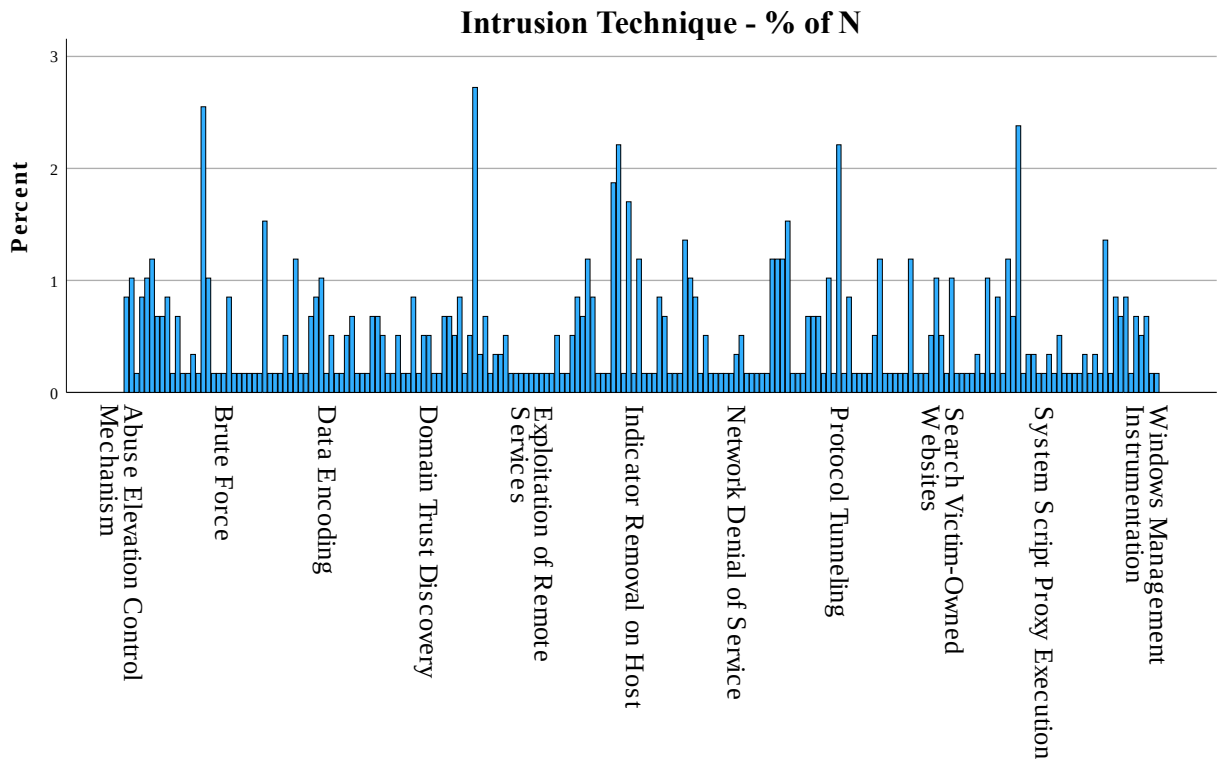


Table 11 below contains the individual total and % of total statistics based on the MITRE CAR intrusion tactics categorization.

Table 11

CAR Intrusion Tactics Frequency Analysis

Intrusion Tactics					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		12	2.0	2.0	2.0
	Collection	29	4.9	4.9	7.0
	Command and Control	36	6.1	6.1	13.1
	Credential Access	53	9.0	9.0	22.1
	Defense Evasion	112	19.0	19.0	41.2
	Discovery	41	7.0	7.0	48.1
	Execution	31	5.3	5.3	53.4
	Exfiltration	17	2.9	2.9	56.3
	Impact	26	4.4	4.4	60.7
	Initial Access	18	3.1	3.1	63.8
	Lateral Movement	15	2.6	2.6	66.3
	Persistence	75	12.8	12.8	79.1
	Privilege Escalation	43	7.3	7.3	86.4
	Reconnaissance	42	7.1	7.1	93.5
	Resource Development	38	6.5	6.5	100.0
	Total	588	100.0	100.0	

Figure 8 below is a graphical representation of Table 11 containing the individual total and % of total statistics of MITRE CAR intrusion techniques.

Figure 8

Bar Chart of CAR Intrusions as % of N

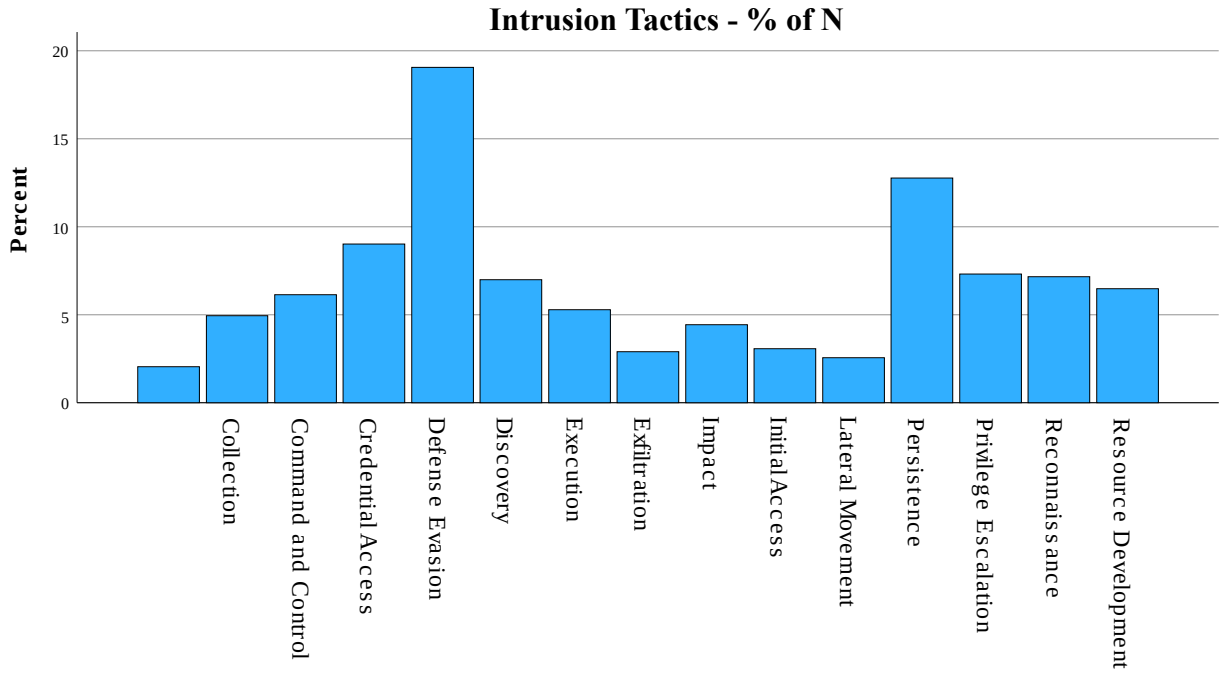


Table 12 below contains individual total and % of total statistics of exploited machine languages based on the CAR detection schema.

Table 12

Exploited Machine Languages - CAR Detection Schema Frequency Analysis

Exploited Machine Languages – CAR Detection Schema				
		Frequency	**Percent**	**Valid Percent**
Valid	**Unknown**	**270**	**45.8**	**45.8**
	CSV	**81**	**13.8**	**13.8**
	YAML	**78**	**13.3**	**13.3**
	Markdown	**78**	**13.3**	**13.3**
	JSON	**81**	**13.8**	**13.8**
	Total	**588**	**100.0**	**100.0**

Table 13 below contains individual total and % of total statistics of exploited machine languages based on the Sigma detection schema.

Table 13

Exploited Machine Languages - Sigma Detection Schema Frequency Analysis

Exploited Machine Languages – Sigma Detection Schema				
		Frequency	**Percent**	**Valid Percent**
Valid	**Unknown**	**280**	**47.6**	**47.6**
	J	**1**	**0.2**	**0.2**
	YAML	**307**	**52.2**	**52.2**
	Total	**588**	**100.0**	**100.0**

Table 14 below contains individual total and % of total statistics of exploited machine languages based on the SIEM detection schema.

Table 14

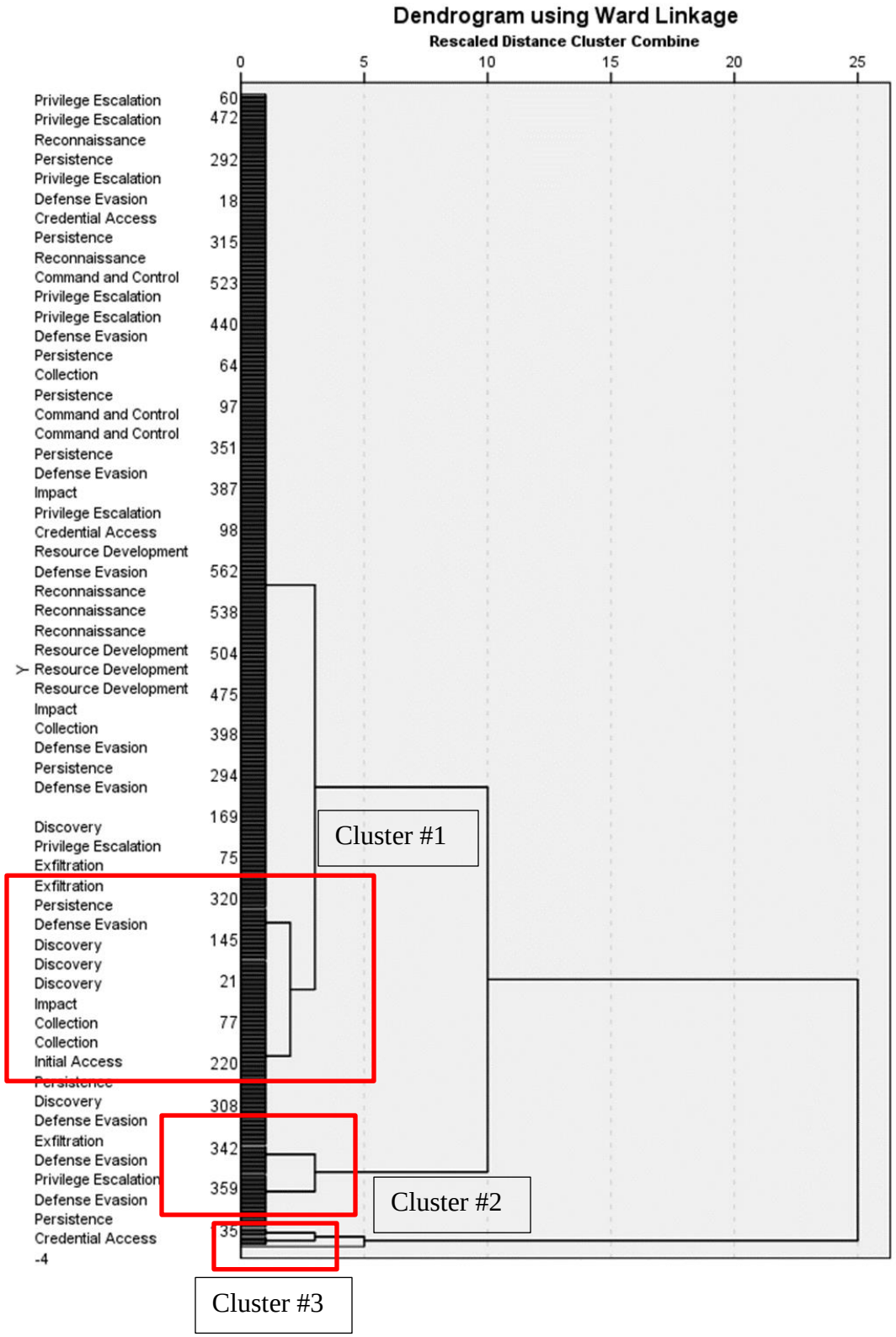
Exploited Machine Languages – SIEM Detection Schema Frequency Analysis

Exploited Machine Languages – SIEM Detection Schema				
		Frequency	**Percent**	**Valid Percent**
Valid	**Unknown**	**109**	**18.5**	**18.5**
	Python	**65**	**11.1**	**11.1**
	TOML	**209**	**35.5**	**35.5**
	JSON	**205**	**34.9**	**34.9**
	Total	**588**	**100.0**	**100.0**

Figure 9 below is the hierarchical cluster dendrogram comparing the proximity of relationship between exploited machine languages organized based on intrusion tactics. The red boxes indicate the three identified clusters based on closest proximity.

Figure 9

Exploited Machine Language Hierarchical Cluster Dendrogram



Results

Hypothesis(es)

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

For RQ1, a *Spearman's rho* correlation coefficient test was calculated to facilitate a bivariate analysis examining the relationship between frequency of malicious software attacks and the diversity of intrusion techniques. A significant positive correlation was found ($r(712) = .891$, $p < .001$), the null hypothesis is rejected and the alternate accepted indicating a significant positive relationship between the dependent and independent variables. Table 15 below is the IBM SPSS output for the RQ1 *Spearman's rho* correlation coefficient test and Figure 10 is the accompanying scatterplot graph.

Table 15

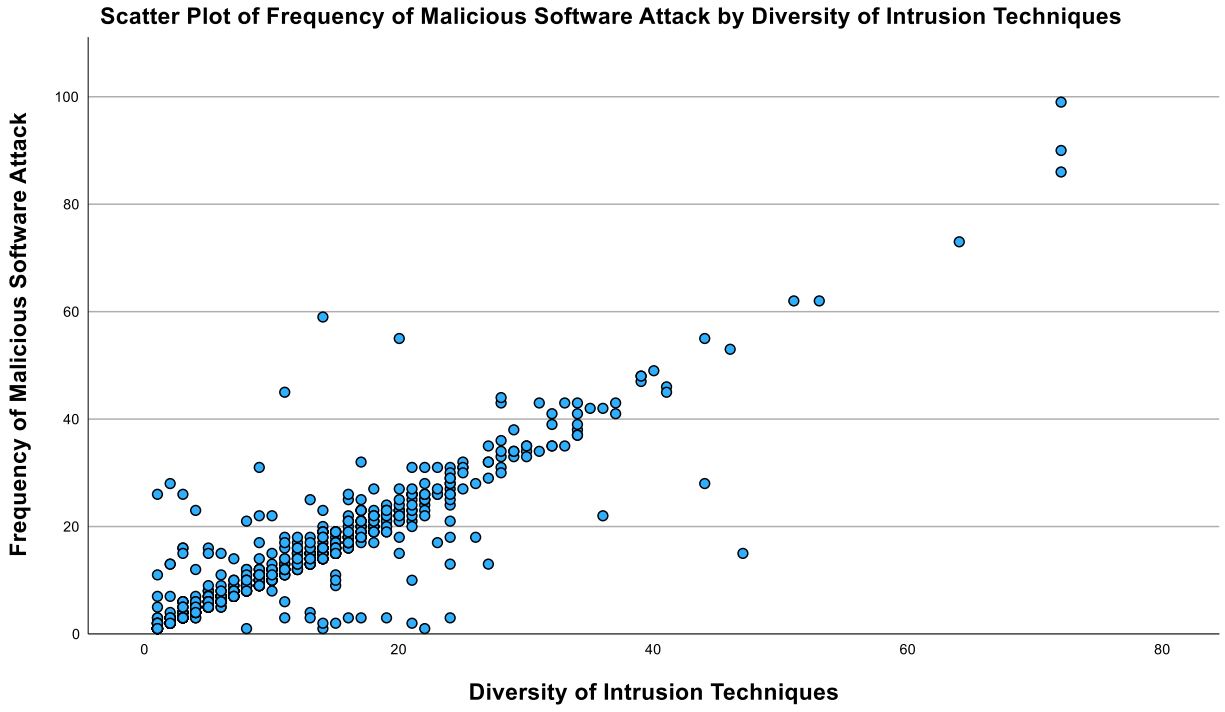
RQ1 Spearman's rho Correlation Coefficient Test

Correlations				
			Frequency of Malicious Software Attack	**Diversity of Intrusion Techniques**
Spearman's rho	**Frequency of Malicious Software Attack**	**Correlation Coefficient**	**1.000**	**.891****
		Sig. (2-tailed)	**.**	**<.001**
		N	**712**	**712**
	Diversity of Intrusion Techniques	**Correlation Coefficient**	**.891****	**1.000**
		Sig. (2-tailed)	**<.001**	**.**
		N	**712**	**712**

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 10

Spearman rho Scatterplot Graph of RQ1 Dependent and Independent Variables



A significant positive correlation indicates that increases in the diversity of intrusion techniques parallels increases in the frequency of malicious attacks as seen in the general trend shown in Figure 10. In the context of RQ1, significant positive correlation between frequency of malicious attacks and the diversity of intrusion techniques is an indicator of the multi-dimensional nature of modern cyber threats where the factors of time and space are coupled with technical multi-functionality to extend the scope of the threat. This multi-dimensionality could demonstrate that a modern cyber threat is inherently multi-pronged (where the attack integrates simultaneous and sequenced time with varied techniques) and able to exploit a multitude of vectors that reduces the effectiveness of single scope cybersecurity policies that focus on specific threat types, behaviors, or signatures. As table 8 illustrates, the malware classification

categorizes 91.5% of documented malicious software in the MITRE Att&ck dataset. And as table 9 illustrates, the top three most prevalent intrusion tactics are defense evasion, discovery, and command and control. These three intrusion tactics organize the remainder of the RQ1 results to illustrate the relationship between the dependent and independent variables.

Defense Evasion

Based on table 9, defense evasion is the most prevalent intrusion tactic comprising 21% of those documented within the MITRE Att&ck dataset. Defense evasion is a tactic defined as "techniques that adversaries use to avoid detection throughout their compromise" (MITRE, n.d.). These techniques include methods that abuse trusted processes for the purposes of hiding malware (MITRE, n.d.). Defense evasion characterizes themes of credential manipulation, alteration of authentication processes, and policy manipulation. Credential manipulation include exploitations of default guest or administrator accounts built into operating systems, local user accounts, and cloud access accounts as well as manipulation of security tokens used to access systems, networks, and databases. Adversaries are capable of creating or impersonating tokens to create logon sessions using a user's legitimate credentials (MITRE, n.d.). Alteration of authentication processes involve utilizing stolen credentials to bypass the normal systemic authentication chains to gain initial access into a digital space or to laterally move from system to system or networks to networks. Policy manipulation focuses on modifying the configuration settings of a domain (MITRE, n.d.). As a domain is the centralized method for managing how computer resources interact within a network (MITRE, n.d.), the ability of the adversary to modify the policies governing domain operations and configurations creates multiple threat vectors.

As examples, the frequency analysis of the MITRE Att&ck dataset (reference Appendix C) reveals that a tool known as Empire is the most prevalent malicious software comprising 1% of those documented. Empire is an "open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub" (MITRE, n.d.). Relative to defense evasion, Empire is used to execute 14 separate intrusion techniques spanning file obfuscation, process injection, modifying file timestamps, proxy code builds, passing stolen password hashes to bypass normal access controls, and injecting malicious payload through the interception of a legitimate program execution path. 14 separate threat groups are also known to have employed Empire in their malicious operations. These threat groups either target specific industries (such as transportation, finance, energy, or telecommunications sectors) or are known, State-sponsored entities (tied to the Islamic Republic of Iran, Russian Federation, and People's Republic of China) primarily conducting cyber-espionage operations. More formidable than Empire in the execution of the defense evasion tactic are malwares known as Cobalt Strike and InvisiMole that comprise 0.9% and 0.8% of documented malicious software respectively. Cobalt Strike is a "commercial, full-featured, remote access tool" (MITRE, n.d.) designed to simulate adversary attacks and post-exploitation actions (MITRE, n.d.). InvisiMole is a "modular spyware program…used to perform post-exploitation activities" (MITRE, n.d.). 22 separate intrusion techniques are associated with each malware encompassing the same range of capabilities as Empire but also expanding into abilities such as acquiring code materials to self-sign malware using legitimate certificates, self-modification (or self-disabling) of security tools to avoid detection, self-modification (or self-disabling) of network firewalls, hiding files and directories to avoid detection, and masquerading malicious tasks or services as legitimate. In addition, Cobalt Strike is affiliated with 20 known threat groups with similar industrial profiles as Empire

and a State-sponsored list heavily populated with People's Republic of China entities while the Russian Federation, Democratic People's Republic of Korea, and the Socialist Republic of Vietnam comprise the remainder.

Discovery

Based on table 9, discovery is the second most prevalent intrusion tactic comprising 19.8% of documented tactics within the MITRE Att&ck dataset. Discovery is defined as "techniques the adversary may use to gain knowledge about the system and internal network" (MITRE, n.d.). Techniques enabling discovery are intended to permit adversaries to "explore what they can control and what's around their entry point in order to discover how it could benefit their current objective" (MITRE, n.d.). Discovery characterizes the theme of probing encompassing account (user, email, cloud, and domain) discovery, browser bookmarks and application windows discovery, infrastructure and services discovery (to include cloud environments), trust and directories discovery, policies and processes discovery, and locations and languages discovery (MITRE, n.d.).

As examples, the frequency analysis of the MITRE Att&ck dataset (reference Appendix C) reveals that InvisiMole and Empire are both prevalent in the execution of the discovery tactic with 15 separately associated intrusion techniques respectively. The presence of InvisiMole, Empire, and Cobalt Strike (with 13 separate associated techniques) as prevalent malicious software in the execution of both defense evasion and discovery starts to establish patterns of utilization for probing and bypassing digital defenses. Ranked with Cobalt Strike at 13 separate techniques are two malicious backdoor trojans known as Epic and Kwampirs. Epic comprises 0.2% of documented malicious software and is linked to a Russian Federation-sponsored threat group targeting government, military, education, research, and pharmaceutical sectors (MITRE,

n.d.). Kwampirs also comprises 0.2% of documented malicious software and is linked to a threat group targeting the health industry and has been detected on high-tech medical devices such as X-rays and MRIs (MITRE, n.d.). Though both are not prevalent in the aggregate count of malicious software, their uniquely tailored implementations span a significant spectrum of discovery techniques.

Command and Control

Based on table 9, command and control comprise 13.2% of documented tactics within the MITRE Att&ck dataset. Command and control consist of "techniques that adversaries may use to communicate with systems under their control within a victim network" (MITRE, n.d.). Techniques enabling command and control "mimic normal, expected traffic to avoid detection" (MITRE, n.d.) to maximize an adversary's ability to stealthily infiltrate a target environment to seize control of it. Command and control characterize the themes of communication and cryptographic exploitation, digital mimicry, and infiltration. Intrusion techniques span protocol exploitation (where the malicious payloads hide in plain sight within applications, web traffic, email exchanges, or domain name server (DNS) communication), data encoding, obfuscation, impersonation, cryptographic concealment, proxy exploitation, and web service relays.

As examples, the frequency analysis the MITRE Att&ck dataset (reference Appendix C) reveals that both Cobalt Strike and InvisiMole are prevalent in the command-and-control tactic with 12 and 10 separately associated intrusion techniques respectively. This prevalence further illustrates the connection between the utilization of these malicious software to the objectives of discovering, infiltrating, and seizing control of target environments that are the objectives of threat actors. Of note are three malicious trojans known as QakBot, RDAT, and SUNBURST. QakBot comprises 0.7% of documented malicious software and ranks behind InvisiMole in

prevalence. QakBot is a "modular banking trojan that…has evolved from an information stealer into a delivery agent for ransomware" (MITRE, n.d.). QakBot has 8 separate techniques for command and control primarily focused on protocol and encoding exploitation. QakBot is linked to a threat group targeting the financial sector specifically those of "English, German, Italian, and Japanese" (MITRE, n.d.) ancestry. RDAT is a backdoor targeting the telecommunications sector (MITRE, n.d.) and comprises 0.2% of documented malicious software with 10 specific command and control intrusion techniques. These techniques are also focused on protocol and encoding exploitation though it is also capable of using steganography to hide malicious information in digital messages (MITRE, n.d.), self-routing communication to alternate channels if the primary channel is compromised and utilizing legitimate symmetric encryption algorithms to conceal its command-and-control traffic. RDAT is linked to a suspected State-sponsored threat group from the Islamic Republic of Iran. SUNBURST is a trojan dynamic link library (DLL) comprising 0.4% of documented malicious software designed "to fit within the SolarWinds Orion software update framework" (MITRE, n.d.). SUNBURST had 9 specific intrusion techniques with the same relative technical profile as RDAT though SUNBURST can also add "random or meaningless data to the protocols used for command and control" (MITRE, n.d.) as a method of preventing decoding, deciphering, and analysis (MITRE, n.d.) of communication traffic. SUNBURST is linked to a State-sponsored threat group associated with the Foreign Intelligence Service of the Russian Federation.

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

For RQ2, a *Spearman's rho* correlation coefficient test was calculated to facilitate a bivariate analysis examining the relationship between the frequency of detection events and the diversity of intrusion techniques. A significant positive correlation was found ($r(169) = .622$, p

< .001), the null hypothesis is rejected and the alternate accepted indicating a significant positive relationship between the dependent and independent variables. Table 16 below is the IBM SPSS output for the RQ2 *Spearman's rho* correlation coefficient test and Figure 11 is the accompanying scatterplot graph.

Table 16

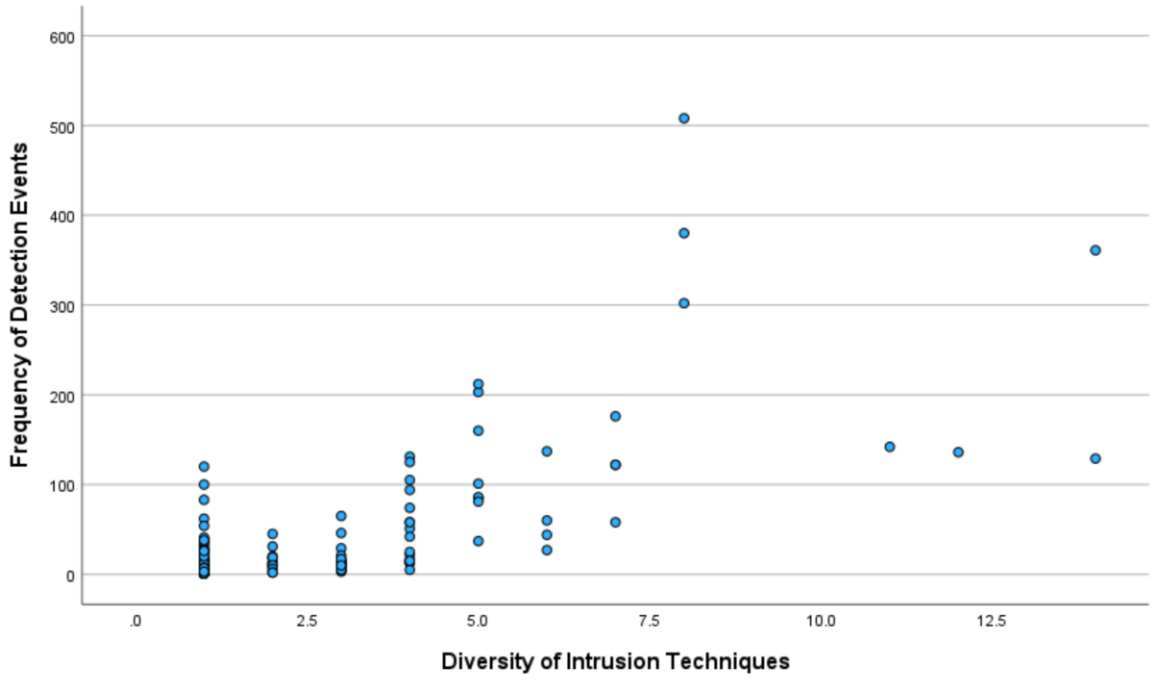
RQ2 Spearman's rho Correlation Coefficient Test

Correlations				
			Frequency of Detection Events	**Diversity of Intrusion Techniques**
Spearman's rho	**Frequency of Detection Events**	**Correlation Coefficient**	**1.000**	**.622****
		Sig. (2-tailed)	**.**	**<.001**
		N	**169**	**169**
	Diversity of Intrusion Techniques	**Correlation Coefficient**	**.622****	**1.000**
		Sig. (2-tailed)	**<.001**	**.**
		N	**169**	**169**

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 11

Spearman rho Scatterplot Graph of RQ2 Dependent and Independent Variables



A significant positive correlation indicates that increases in the diversity of intrusion techniques parallels increases in the frequency of detection events as seen in the subtle distribution shown in Figure 11. In the context of RQ2, the correlation between frequency and diversity does not necessarily indicate an increase in the *probability* of detection but rather, that a point of detection has the *potential* to be connected to a complex series of intrusion points originating from a single malicious actor. Complexity and diversity most likely influence the scale (and scope) of modern cyber threats demonstrating a potential requirement for emergent cybersecurity policies to inherently consider cyber intrusions as interrelated (and interconnected) events rather than isolated attacks. As table 11 illustrates, the top three most prevalent intrusion

tactics are defense evasion, persistence, and credential access. These three intrusion tactics organize the remainder of the RQ2 results.

Defense Evasion

Based on table 11, defense evasion is the most prevalent intrusion tactic comprising 19% of those documented within the MITRE CAR dataset. As with RQ1, defense evasion is a tactic defined as "techniques that adversaries use to avoid detection throughout their compromise" (MITRE, n.d.). Defense evasion exploits the YAML and Tom's Obvious Minimal Language (TOML) machine languages, the Javascript Object Notation (JSON) and Comma Separated Values (CSV) data exchange formats, and the Python programming language. Figure 9 amplifies the significance of this prevalence as cluster #1 indicates a relationship across exploited machine languages between it and the tactics of discovery, impact, collection, and initial access while cluster #2 indicates a relationship between it and privilege escalation. Together, clusters #1 and #2 illustrate the multi-variate (and interconnected) nature of exploitation operations as securing specific machine languages or mitigating a specific intrusion might not inherently reduce the overall threat.

Of the 112 documented intrusion incidences within the CAR dataset, the most prevalent (at 12.5% or 14 incidences) comes from the "system binary proxy execution" intrusion technique. The system binary proxy execution intrusion technique bypasses "process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise, trusted, binaries" (MITRE, n.d.). The technique contains sub-techniques for exploiting HTML code, Microsoft Windows utilities (to include command line installers), DLL registration services, code injectors, and Microsoft console services. This specific technique has been linked to a State-sponsored threat group affiliated with the Reconnaissance General Bureau of the

Democratic People's Republic of Korea. The next most prevalent technique is "hide artifacts" (at 9.8% or 11 incidences) where adversaries "attempt to hide artifacts associated with their behaviors to evade detection" (MITRE, n.d.). The sub-techniques are designed to hide malicious behavior in files and directories, user accounts, Microsoft Windows scripting language, master file tables, malicious virtualized instances running on hosts, and inbound email rules. This specific technique is not associated with a particular threat group, but it is difficult to mitigate through preventative measures as the target environment must be able to detect the abuse (MITRE, n.d.).

Persistence

Based on table 11, persistence comprises 12.8% of documented tactics within the MITRE CAR dataset. Persistence is defined as "techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access" (MITRE, n.d.). Techniques enabling persistence are intended to permit adversaries to "maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code" (MITRE, n.d.). Persistence characterizes themes of account manipulation, alteration of authentication processes, and initiation scripts. Persistence exploits YAML, TOML, JSON, CSV, and Python. Of the 75 documented intrusion incidences within the CAR dataset, the most prevalent (at 17.3% or 13 incidences) comes from the "event triggered execution" intrusion technique. Event triggered execution is where adversaries establish persistence "using system mechanisms that trigger execution based on specific events" (MITRE, n.d.). This technique possesses a series of sub-techniques spanning changing file associations, execution of screensaver functions, Microsoft Windows subscription management functions, DLL exploitation, event monitor exploitation, and PowerShell exploitations. Event triggered

execution is a difficult technique to mitigate through preventive measures as the target environment must be able to detect the abuse (MITRE, n.d.). The next most prevalent intrusion technique is "boot or logon autostart execution" (at 14.6% or 11 incidences) where adversaries "configure system settings to automatically execute a program during system boot or logon" (MITRE, n.d.). The sub-techniques exploit registry keys, authentication packages for DLL execution, security support providers for DLL execution, print processing DLLs, and MS Windows active setup processes. This technique is also difficult to mitigate through preventive measures as the target environment must be able to detect the abuse (MITRE, n.d.).

Credential Access

Based on table 11, credential access comprises 9.0% of documented tactics within the MITRE CAR dataset. Credential access "consists of techniques for stealing credentials like account names and passwords" (MITRE, n.d.). Credential access techniques are intended to "give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals" (MITRE, n.d.). Credential access characterizes the theme of identity theft and exploits YAML, TOML, JSON, CSV, and Python. Figure 9 amplifies the significance of credential access as cluster #3 is centered on this specific tactic and is comprised of a closely related set of exploited machine languages. Of the 53 documented intrusion incidences within the MITRE CAR dataset, "OS credential dumping" is the most prevalent technique (at 16.98% or 9 incidences). OS credential dumping is a technique where adversaries attempt to "dump credentials to obtain account login and credential material, normally in the form of a has or a clear text password" (MITRE, n.d.). The sub-techniques exploit security account managers and local security authorities, cached domain credentials, domain controller API processes, root privilege processes, and password stores. A myriad of

threat actors (both State-sponsored and malware families) is known to use OS credential dumping as an exploitation technique. The next more prevalent technique (at 15.09% or 8 incidences) is "unsecured credentials" where adversaries "search compromised systems to find and obtain insecurely stored credentials" (MITRE, n.d.). Sub-techniques exploit credentials that are stored in files and registries, command line histories, private keys that are stored in secured shell (SSH) directories, group policy preferences, and containerized APIs. This technique has a series of potential mitigations spanning properly configured active directories and operating systems, file auditing, network traffic filtering, robust password policies, and proper account management.

Risk

Table 17 below are the descriptive statistics (N = 559) of the CAPEC dataset based on the mechanisms of attack categorizations.

Table 17

CAPEC Mechanisms of Attack Frequency Analysis

Category Name					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**Abuse Existing Functionality**	**93**	**16.6**	**16.6**	**16.6**
	Collect and Analyze Information	**112**	**20.0**	**20.0**	**36.7**
	Employ Probabilistic Techniques	**9**	**1.6**	**1.6**	**38.3**
	Engage in Deceptive Interactions	**80**	**14.3**	**14.3**	**52.6**
	Inject Unexpected Items	**72**	**12.9**	**12.9**	**65.5**
	Manipulate Data Structures	**4**	**.7**	**.7**	**66.2**
	Manipulate System Resources	**98**	**17.5**	**17.5**	**83.7**
	Manipulate Timing and State	**6**	**1.1**	**1.1**	**84.8**
	Subvert Access Control	**85**	**15.2**	**15.2**	**100.0**
	Total	**559**	**100.0**	**100.0**	

Table 18 below are the descriptive statistics of CAPEC cyber intrusion likelihood of attack.

Table 18

CAPEC Cyber Intrusion Likelihood of Attack

Likelihood Of Attack					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High	131	23.4	23.4	23.4
	Low	96	17.2	17.2	40.6
	Medium	118	21.1	21.1	61.7
	Unknown	214	38.3	38.3	100.0
	Total	559	100.0	100.0	

Table 19 below are the descriptive statistics of CAPEC cyber intrusion typical severity.

Table 19

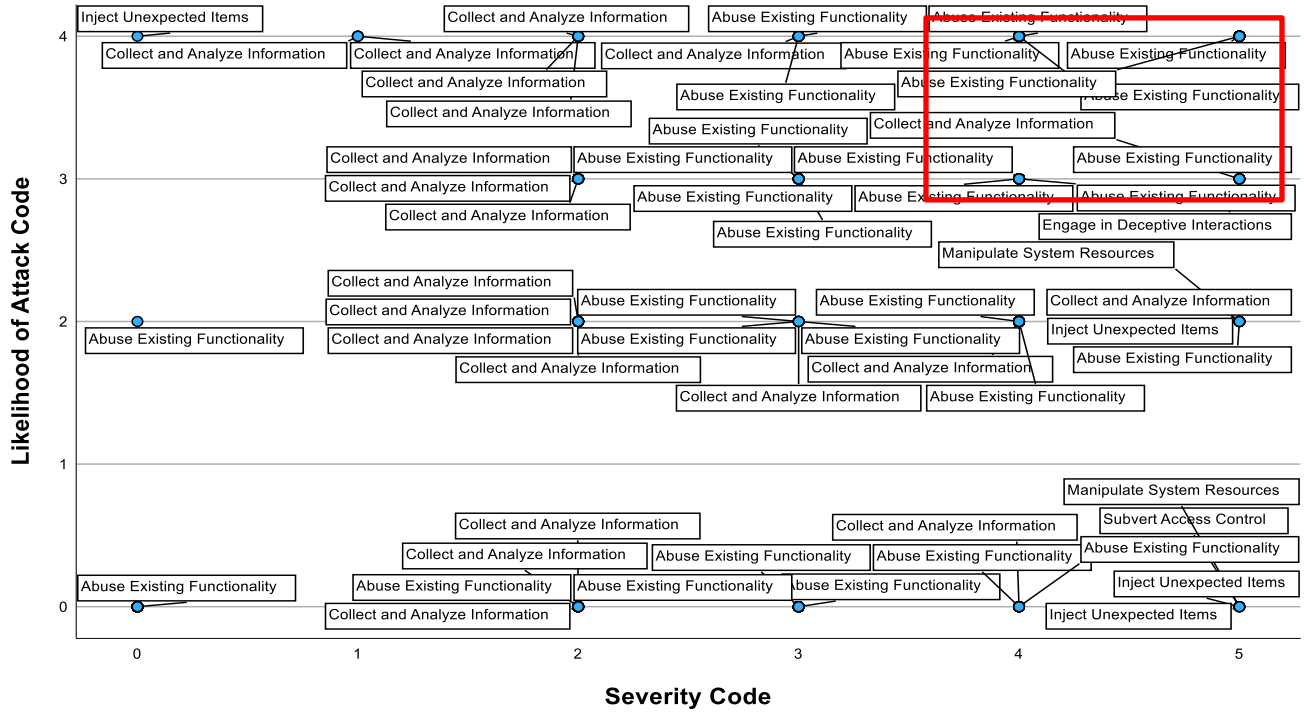
CAPEC Cyber Intrusion Typical Severity

Typical Severity					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High	211	37.7	37.7	37.7
	Low	103	18.4	18.4	56.2
	Medium	112	20.0	20.0	76.2
	Unknown	70	12.5	12.5	88.7
	Very High	59	10.6	10.6	99.3
	Very Low	4	.7	.7	100.0
	Total	559	100.0	100.0	

Figure 12 below is the scatterplot of the likelihood of attack compared to severity of the attack. The highlight box indicate the mechanisms assessed with a “high” likelihood of attack and a “very high” severity.

Figure 12

CAPEC Scatterplot Comparing Likelihood of Attack with Severity



As presented in Chapter 3, risk is calculated as *risk = likelihood of occurrence x severity of risk* (Zahid et al, 2020). Based on table 17, the "collect and analyze information" categorization is the most prevalent mechanism of attack at 20%. This mechanism is the "gathering, collecting, and theft of information by an adversary" (CAPEC, n.d.) to make inferences about the weaknesses, vulnerabilities, or techniques that could assist the adversary in exploiting the target (CAPEC, n.d.). Techniques associated with this mechanism are "excavation", "interception", "footprinting", "fingerprinting", "reverse engineering", protocol analysis", and "information elicitation" (CAPEC, n.d.) where the attack pattern with the highest assessed risk is the "retrieve embedded sensitive data". This pattern has a "high" likelihood of attack and a "very high" severity and is based on an adversary examining a target to "find sensitive data that has been embedded within it" (CAPEC, n.d.) as a prelude to a more extensive

attack (CAPEC, n.d.). The “accessing/intercepting/modifying HTTP cookies”, “WSDL scanning”, and “shoulder surfing” are three other patterns assessed as “high” likelihood of attack and “high” severity. The “assessing/intercepting/modifying HTTP cookies” mines HTTP cookies for potentially sensitive data, intercepts data from client to server or modifies a cookie's content before it is sent back to the server (CAPEC, n.d.). The objective of this pattern is to convince the target server to operate on falsified information that the adversary creates (CAPEC, n.d.). The “WSDL scanning” pattern probes the WSDL interface of a web service to provide detailed information about the ports and bindings available to consumers (CAPEC, n.d.) that the adversary could use to conduct a denial-of-service attack or gain illegal access to database records (CAPEC, n.d.). The “shoulder surfing” pattern is where an “adversary observes an unaware individual's keystrokes, screen content, or conversations with the goal of obtaining sensitive information” (CAPEC, n.d.) for financial, personal, political, or other gains (CAPEC, n.d.).

Based on table 17, the “manipulate system resources” is the next most prevalent mechanism of attack at 17.5%. This mechanism is a “broad class of attacks wherein the attacker is able to change…aspects of resources’ state or availability” (CAPEC, n.d.) to affect system behavior or integrity (CAPEC, n.d.). Techniques associated with this mechanism are “software integrity attack”, “hardware integrity attack”, “infrastructure manipulation”, “file manipulation”, “configuration/environment manipulation”, “obstruction”, “modification during manufacture”, “manipulation during distribution”, “malicious logic insertion”, and “contaminate resource” (CAPEC, n.d.). The “leverage executable code in non-executable files”, “poison web service registry”, and “manipulating writeable configuration” are assessed as the highest risk with “high” likelihood of attack and “very high” severity. The “leverage executable code in non-executable

files" pattern exploits the trust of configuration and resource files (CAPEC, n.d.) for the purposes of executing "malicious code directly or manipulate the target process…to execute based on the malicious configuration parameters" (CAPEC, n.d.). The "poison web service registry" pattern can redirect a "service requester to a malicious service provider, provide incorrect information in schema or metadata, and delete information about service provider interfaces" (CAPEC, n.d.). The "manipulating writeable configuration" pattern enables the adversary to modify manually edited files to "give unauthorized access directly to the application" (CAPEC, n.d.) as if the adversary were an authorized user.

Based on table 17, "abuse existing functionality" is the third most prevalent mechanism at 16.6%. This mechanism "manipulates one or more functions of an application in order to achieve a malicious objective…or to deplete a resource to the point that the target's functionality is affected" (CAPEC, n.d.). Techniques associated with this mechanism are "interface manipulation", "flooding", "excessive allocation", "resource leak exposure", "functionality misuse", "communication channel manipulation", "sustained client engagement", "protocol manipulation", and "functionality bypass". The "overflow binary resource file", "string format overflow in syslog", "manipulating web input to file system calls", "overflow buffers", and "path traversal" are assessed as the highest risk with "high" likelihood of attack and "very high" severity. The "overflow binary resource file" pattern exploits the vulnerability in the handling of binary resources enabling adversarial "access to the execution stack and execute arbitrary code in the target process" (CAPEC, n.d.). The "string format overflow in syslog" pattern permits the adversary to "inject malicious format string commands into the function call" (CAPEC, n.d.) for software exploitation at the root of a syslog (CAPEC, n.d.). The "manipulating web input to file system calls" pattern enables the adversary "to gain access to…areas of the file system that the

target did not intend to make accessible" (CAPEC, n.d.) through exploitation of system calls to the operating system (CAPEC, n.d.). The "overflow buffers" pattern targets improper or missing boundary checks in buffer operations (CAPEC, n.d.) to permit the adversary to "write past the boundaries of allocated buffer regions in memory" (CAPEC, n.d.) which can cause crashes or redirection (CAPEC, n.d.). The "path traversal" pattern exploits "insufficient input validation…to obtain access to data that should not be retrievable by ordinary well-formed requests" (CAPEC, n.d.).

Amplification of risk data comes through an examination of the 34 patterns assessed as "high" likelihood of attack and "very high" severity (reference Appendix D). Aside from the nine associated with the three most prevalent mechanisms, the "inject unexpected items" is the mechanism that has the most percentage of highest risk patterns (at 29.4% or 10 patterns). This mechanism is the control or disruption of target behavior through crafted data or "the installation and execution of malicious code on the target system" (CAPEC, n.d.). The intent of this mechanism is to cause a target application to perform unintended steps or to enter an unstable state (CAPEC, n.d.) as adversaries place instructions within the malicious code to force targeted applications to follow their commands. The techniques associated with this mechanism are "XSS targeting non-script elements", "file content injection", "manipulating writeable terminal devices", "cross-site scripting (XSS)", "XQuery injection", "SQL injection through SOAP parameter tampering", "DOM-based XSS", "reflected XSS", and "stored XSS". Of note is the prevalence of cross-site scripting (XSS) attack techniques exploiting web browser content and web applications through the insertion of malicious code (CAPEC, n.d.). XSS attacks exploit a core foundation of the IoT itself so even though "inject unexpected items" comprises only 12.9% of the total number of intrusion mechanisms in table 17, it is worth noting its significance. The

"subvert access control" mechanism has the second most prevalent number of patterns with the highest assessed risk (at 23.5% or 8 patterns). This mechanism exploits the weaknesses, limitations, and assumptions in identity and authentication systems to include accessing their resources and functionality (CAPEC, n.d.). This mechanism results in the "complete subversion of any trust the target system may have in the identity of any entity with which it interacts, or the complete subversion of any control the target has over its data or functionality" (CAPEC, n.d.). The techniques associated with this mechanism are "subverting environment variable values", "using malicious files", cross site request forgery", target programs with elevated privileges", "manipulating user-controlled variables", "adversary in the middle (AiTM)", "session hijacking", and "adversary in the browser (AiTB)". This mechanism is much more varied in how it executes exploitation but, in general, it is focused on assuming control, or altering, the behavior-based processes of the target through the subversion of the implicit trust model. As foundations of trust are critical for IoT stability and the maintenance of legitimate data exchanges, it is worth noting its significance as it is the fifth most prevalent mechanism in the aggregate count (at 15.9%) based on table 17. The "engage in deceptive interactions" has the third most prevalent number of patterns with the highest assessed risk (at 17.6% or 6 patterns). This mechanism seeks to "convince the target that it is interacting with some other principle and…take actions based on the level of trust that exists between the target and the other principle" (CAPEC, n.d.). The focus of this mechanism is content falsification so that "the target will incorrectly trust the legitimacy of the content" (CAPEC, n.d.). The techniques associated with this mechanism are "leveraging/manipulating configuration file search paths", "pharming", "phishing", "redirect access to libraries", "action spoofing", and "DNS rebinding". This mechanism impersonates or manipulates legitimate workflows, functions, and data objects to

convince a target to interact with the adversary for the purposes of granting access, assuming control, or conducting illicit data harvesting. It is worth noting its significance as it is the fourth most prevalent mechanism in the aggregate count (at 16.6%) based on table 17.

CHAPTER FIVE: CONCLUSIONS

Overview

The outcomes of this research have provided insights into the relationship between malicious software attacks, intrusion techniques, and intrusion detection events. Given the limitations of current research, the results are interpreted with a measure of caution. The research results indicated a significant positive correlation between the frequency of malicious software attacks and the diversity of intrusion techniques. Furthermore, a significant positive correlation was demonstrated between the frequency of detection events and the diversity of intrusion techniques. This chapter reflects on the research results and offers potential implications based on the interpretation of those results. Machine cognition and the social IoT replicates societal concepts which have significant influence on physical and digital world dynamics. This quantitative study examined the complex nature of modern cyber threats to propose the establishment of cyber as an interdisciplinary field of public policy initiated through the creation of a symbiotic cybersecurity policy framework. The academic contribution of this research project is the fusion of humanistic principles with Internet of Things (or IoT) technologies that alters our perception of the machine from an instrument of human engineering into a thinking peer to elevate cyber from technical esoterism into an interdisciplinary field of public policy. This impacts and disrupts future research paradigms (particularly in the public policy, behavioral sciences, social sciences, and cyber domain) as the IoT and adaptive modern technologies has enabled a potentially emergent concept of a machine society that is equal to (but independent of) human society. The contribution to the US national cybersecurity policy body of knowledge is a unified policy framework (manifested in the human-cognitive machine symbiotic cybersecurity policy triad comprised of digital identity legitimization, trust and

positive reputation, and ethical motivation) that could transform cybersecurity policies from network-based to entity-based. The chapter ends with recommendations for future research.

Discussion

The purpose of this study is to postulate a design framework for symbiotic cybersecurity policies incorporating cognitive machine individualism to enhance the implementation of human-machine teaming (HMT) in the preservation of IoT integrity. The problem is that current US national cybersecurity policies operate on the principle of implicit trust that neither enables machines to verify their identities before a data transaction is initiated nor accounts for their behavioral intent. Current network-based cybersecurity has created a fragmented policy approach, policy design, and implementation methodologies as organizations subjectively apply cybersecurity principles based on their specific technical architecture. Cognitive machine self-determinative capabilities are not accounted for in current cybersecurity policies as the machine is not perceived to be an equal partner. Research and the available literature indicate an increasingly complex scale of security dynamics as adaptive, complex attack models dilute cybersecurity situational awareness which hampers human-centric response and remediation methodologies (Andrade, 2019).

Discussion: Research Questions

RQ1: *What are the important factors for the prevention of malicious software exploitation in the design of identity-based cognitive machine symbiotic cybersecurity policies?*

For RQ1, the analysis indicates a significant positive correlation between the frequency of malicious software attacks and the diversity of intrusion techniques. The risk comparative amplifies this relationship as the three highest risk mechanisms involve controlling (or modifying) target behavior through the installation of malicious code, subverting identity and

authentication systems, and exploiting trust through deception operations. The descriptive statistics indicate that the highest concentration of intrusions is centered on tactics associated with bypassing existing cybersecurity defenses, knowledge-gathering of targeted environments, and obtaining control of targeted environments. Bypassing existing cybersecurity defenses has the highest percentage of occurrences and involves techniques related to credential manipulation, alteration of authentication processes, and policy manipulation. In credential manipulation alone, malicious threats can forge security tokens using legitimate user credentials or manipulate user accounts to bypass cybersecurity measures and gain access to a target. The work of Chia and Chin (2020) reflects this impersonation schema in stating that security breaks when the impersonator is "able to fool the verifier into accepting it's proof of identity with non-negligible probability" (Chia and Chin 2020, p. 61716). The research contextualizes the work of Pal et al (2018) where there must be "an emphasis on being able to link identities…uniquely to a particular entity" (Pal et al 2018, p. 48).

The true impact of the IoT is not the deployment of advanced technologies to create persistent data and information streams but the replication of real-world social relationships (encompassing both humans and machines) with their inherent bias, pre-conceived intent, and complicated sociological dynamics. The IoT is an ideas-based ecosystem manifesting as technological innovation where those ideas are leveraged to extend influence, alter behavior, or impose authorities and dominance. Increasing machine cognition increases their risk exposure to societal ideas; as cognition implies self-determinative capabilities, exposure to ill-advised bias, prejudices, and authoritative machinations means that the behavior of machines could be negatively swayed or ideologically influenced. Modern cybersecurity policies lack a socio-psychological framework to mitigate such emergent possibilities as technologies are still treated

as isolated systems and machines are perceived as instruments rather than as an increasingly cognitive actor capable of independent decision-making. Identity-based cognitive machine symbiotic cybersecurity policies are an initial proposal towards an interdisciplinary formulation of IoT cybersecurity policies leveraging the HMT strengths of technological innovation and social symbiosis. Rezvanian et al (2018) state that digital world social dynamics fluctuate in a non-deterministic and unpredictable fashion (Rezvanian et al, 2018) as "shared items and activities of audiences…may change over time and have an impact on the behavior of other users' activities" (Rezvanian 2018, p. 279). IoT data exchanges spread influence and ideas as its persistent data environment is built on a societal relationship model where machines are increasingly capable of comprehending ontologies within the data. Cognitive machines can interpret context within the content to independently build awareness and understanding. Michie et al (2017) amplify this in stating that a system is artificially intelligent because it expresses traits "such as advanced reading ability and significant domain understanding" (Michie et al 2017, p. 7). The implicit trust paradigm of current cybersecurity policies does not account for these IoT social network dynamics as modern cyberspace is essentially a landscape of persistent digital communication. In the physical world, trust is not automatically granted between two parties particularly if those two parties are not acquainted with each other. Establishing trust in the physical world requires the ability to verify the identities of the other party, confirm that interactions and exchanges are legitimate, and understanding the motivations behind the exchanges. There is a social and behavioral construct behind the establishment of trust in the physical world. In the digital world, the IoT has steadily replicated similar social structures between digital entities yet there are no consistent policy-driven processes for establishing trust when humans and machines are the two interactive parties. The lack of an interdisciplinary

approach to cybersecurity policies creates blind spots because we underestimate (or underappreciate) the strength of the cognitive machine as a partner in IoT defense as H2M and M2M interactions are not framed as social relationships. The technical nature of current cybersecurity policies emphasizes security through technical solutions rather than harnessing relational strength between organic and synthetic entities. Ozkaya (2020) supports an interdisciplinary approach (where HMT trust is built at the intersection of technology and behavioral science) as designing trustworthy HMTs "has to start from an explicit and consciously designed inclusion of human aspects" (Ozkaya 2020, p. 4). Identity-based cognitive machine symbiotic cybersecurity policies could inform the design of a consistent conceptual and theoretical framework for defining human and cognitive machine digital identities based on the social interactive aspects of HMTs that are anchored in ethical (and moral) motivations.

The one-to-one relationship between digital entities and their identities is attributional; for cognitive machines, it indicates that cybersecurity policies designed to prevent (or mitigate) the threat from impersonating their identities must contain a set of data attributes imparting machine distinctiveness. Distinctiveness is the recognition mechanism for IoT entities since activities within the digital space are transactional as parties must trust that exchanges are occurring between legitimate entities. The research indicates that cyber threats utilize sophisticated methods to gain trust through impersonation, alteration or manipulation of identity credentials, account privileges, or policy guidelines. Mohammadi (2019) states that trust includes subjective components (Mohammadi, 2019) and that limiting this subjectiveness requires attributes to "bring an objective view on trustworthiness" (Mohammadi 2019, p. 68). A consistent symbiotic cybersecurity policy framework should inform the attributional (enforced through cryptographic signatures) architecture required to uniquely identify humans and

cognitive machines to prevent (or mitigate) impersonations. Having a cryptographically signed, attributional architecture applicable for digital uniqueness can create the process steps and workflows for establishing identity legitimacy while stimulating further conversation on identity ownership, enforcement of digital ethics, continued incorporation of reputational engines to augment identity legitimization, and the psychology of machine motivations. The study concludes that a common digital identity ontological (or terms of reference) structure, shared technical attribute schema, and business processes for validating and preserving digital legitimacy are the factors that could potentially prevent (or mitigate) ongoing malicious software exploitations.

RQ2: *Why is cognitive machine SSI a contributor to cohesive cybersecurity policies?*

For RQ2, the analysis indicates a significant positive correlation between the frequency of detection events and the diversity of intrusion techniques. Tables 12-14 indicate that YAML, TOML, CSV, and JSON are highly exploited languages (or formats) which is noteworthy as these languages are open source, commercially accessible, and prevalent across the span of the IoT. This is important to understand as machines "talk" in these languages (or data formats) which includes the transmission of credentials. In traditional identity management systems, a central identity provider creates, manages, and maintains identity information for digital users (Moreno, 2021). These third parties utilize their own identifiers as there is "no universally unique identifier…used as a standard interoperable mechanism" (Naik 2020, p. 2). The lack of interoperability and an over-reliance on centralized data repositories exposes these third parties to illicit operations due to the "complex, inconsistent, tangled, and insecure web of digital identity practices" (Soltani 2021, p. 1).

SSI is based on the premise that the owners of digital identities should not cede control to centralized providers in the era of big data (Sedlmeir, 2021). SSI is a mechanism for integrity checks as its architecture is comprised of "a set of community-sourced ethical principles that pertain to digital identities, privacy rights, and personal information" (Sedlmeir 2021, p. 607). Central to SSI is the unique identifier (in the form of a DID). Applied to cognitive machines, the DID provides a data-oriented method for a cognitive machine to present its credentials in P2P exchanges with the proper documentation that it can self-sign. The work of Sheron et al (2019) proposed a decentralized security framework based on device verification and message authentication (Sheron et al, 2019) corresponding to Fedrecheski et al (2020) whose work states that SSI is defined as a set of name-value attributes "that span a range of decentralized domains" (Fedrecheski et al 2020, p. 1). Aside from the technical characteristics of SSI, the premise of decentralizing (and empowering self-ownership of) digital identity credentials is a consistent framework for cybersecurity policy designers as its fundamentals are oriented around claims and proof. If the owner of an SSI makes certain claims about their digital identity, credentials must be produced to validate those claims to prove the owner's identity. This is a repeatable methodology that is fundamentally easy to understand and not dependent on organization specific network configurations. The fragmented nature of traditional identity management systems is exacerbated within the heterogeneous nature of the IoT as lack of interoperability limits the inheritance of security features and processes across disparate user groups. The analysis suggests that the exploitation of specific machine languages is not a limiting factor for cyber threats as the targeted languages are commonly accepted. Moreover, the diversity of intrusion techniques means that malicious software conducts operations in multiple simultaneous or parallel methods where individually detected events might simply be a portion of an

extensive, complex attack. Multi-faceted and multi-layered complex attacks take advantage of persistent IoT connectivity for propagation, exploitation, and continuance that make it difficult to discover patterns and associations. These difficulties are further exacerbated as current cybersecurity policies tend to posture mitigation and remediation responses based on simple signature detection and isolated network penetration schemes. As threats take advantage of the IoT to spread themselves widely using multiple avenues and methodologies, the vulnerabilities associated with widely used machine languages and data formats has exposed digital resources to a threat complexity that diminishes the power of third-party identity verifiers. The study concludes that cognitive machine SSI is a mechanism to reduce the fragmentation of identity credentials and credentials management. The consistency of the SSI identity verification process (and the concept of digital distinctiveness) can enable HMT digital symbiosis for the purposes of aligning humans and cognitive machines towards the same goals of defending the IoT against malicious actors as both partners can share the same framework for recognizing and authenticating their personal identities.

Discussion: Cyber Policy as an Interdisciplinary Field of Public Policy

Yi (2023) stipulates that the principles of public policy thoughts are "contingent on metaphysical and conceptual answers and consciousness to formulate and advance policy thinking" (Yi 2023, p. 6). The author identifies the five principles of policy thought as policy statism, policy goodness, policy balance, policy practicality, and policy interpenetration between humans and non-humans (Yi, 2023). From the philosophical and scholarly perspective, the social characteristics of the IoT and the entities that interact within it have transcended the technical esoterism of traditional cybersecurity (and cyber-related) policies. Due to the social IoT and the presence of cognitive machines, cyber policies require broader reflection within the

public policy community as the acceleration of digital cognition impacts the philosophical and ideological underpinnings of public policies. The social IoT has organic and synthetic cognitive voices, both capable of expressing themselves within the digital world with the synthetic voice increasingly capable of influencing the expressive capabilities of the organic one. For the public good (and maintaining ideological balance), there must be recognition that public policies are at a transition point where the digital public square is a tangible reality that is more than a collection of technological widgets. Steed (2019) expounds on the concept of cyber sovereignty that is intertwined with specific national foreign policy approaches to assert the rights of national governments in controlling the internet (Steed, 2019). Cyber sovereignty is further associated with economic security and social stability as cyber is a domain to "interfere in the internal political affairs of other countries, to attack other countries' political systems, incite social unrest…and other such activities gravely harm national political security and users' information security" (Steed 2019, p. 65).

Cyber policy as an interdisciplinary field of public policy is a concept that is not without precedence as the digital world encapsulates the interdisciplinary elements of all other public policy fields due to the growth of the social IoT and the inception of the cognitive machine. Social, economic, foreign, and national security public policies are reflected in (or affected by) the presence of cyber yet their policy aspects do not integrate cyber as a fundamental element of their design architecture. The digital public square is equal to the physical public square as public policy paradigms co-habitat with the technological characteristics of the social IoT. In effect, cyber integrates the interdisciplinary nature of public policies within the IoT yet cyber policies are not formulated with interdisciplinary methodologies nor is cyber considered a domain that public policies should either extend into, or elevate as, a public policy discipline.

Vectoring cyber policies away from technical esoterism parallels the argument from Austin (2021) where “social considerations are..evident in modern approaches to cyber security, they have rarely been analyzed as part of a complex socio-technical system” (Austin 2021, p. 128). As the digital world was “designed so all citizens of the world could have access to a gateway of communication” (Fowler 2022, p. 59), the IoT encapsulates democratic principles that are not informed by (or governed under) the current philosophical approaches to public policies. Cyber policy as an interdisciplinary field of public policy is a paradigm shift for informing Governments and public sector institutions on how to “defend our needs and consider our rights and freedoms to express ourselves” (Fowler 2022, p. 59) within (and in relations to) the digital world. For US public policy thinkers and designers (particularly in the national security field), cyber policy as an interdisciplinary field of public policy reflects a perspective of information warfare that focuses on “shaping perceptions, beliefs, and ultimately decisions and actions of an adversary” (Lawson 2020, p. 169). Public policies are designed to achieve specific societal effects, actions, and behaviors. As the social IoT does not adhere to specific geopolitical and ideological boundaries, US public policy scholars must appreciate the potentiality that adversarial nation-states will extend their public policy paradigms into cyberspace for the purposes of aligning IoT behaviors and culture towards their strategic and ideological objectives.

The cognitive machine is facilitating an evolution of the cyber domain requiring a revolution in the scholarly foundation of public policies as the cognitive machine is a public figure (manifested as a digital entity) that is capable of both interpreting policy context and (increasingly) shaping future policy design and decisions. The cognitive machine has the potential to inform, advise, and influence policymakers and (with sophisticated ML) craft its own public policies for implementation within the digital world. Whyte and Mazanec (2023) state

that social and cultural institution shape the digital world (Whyte and Mazanec, 2023) that reflects "our geopolitics, our economic systems and behaviors, and those inherent sociopolitical insecurities" (Whyte and Mazanec 2023, p. 320). The interactions between organic and synthetic entities in the IoT expands the traditional human-centric public policy approaches and requires policy scholars and philosophers to ask the question of whether cognitive machines are bound under (or compelled by) our public policies. If the answer is no, then the machine is potentially free to govern itself under a societal framework of its own invention. If the answer is yes, then the expansiveness of the digital world cannot be encompassed as a sub-set of traditional public policy disciplines but rather, cyber must be elevated to its own interdisciplinary field as it must accommodate (and account for) two intelligent communities, one organic and one synthetic.

Discussion: Human-Cognitive Machine Symbiotic Cybersecurity Policy Triad

The human-cognitive machine symbiotic cybersecurity policy framework is anchored by a circuitous triad where digital identity legitimization reinforces trust and positive reputation based on the ethical motivation of interactive IoT partners. A symbiotic cybersecurity policy framework relies on identity proofing where digital interactive partners can prove their physical identities and the "existence of necessary information…as genuine and trustable" (Shibuya 2020, p. 89). Self-determination Theory (SDT) postulates that "intrinsically motivated behavior is self-determined" (Oppl 2022, p. 8) where values of behavior are internalized based on how well basic psychological needs are met (Oppl, 2022). The consequence of cognitive machine autonomous capability is that "social and psychological factors are considered to a greater extent in autonomy" (Demir et al 2021, p. 696) than in ordinary automation as the machine can express open-ended capabilities of emotions and motivations (Burden and Saven-Baden, 2019). Autonomy implies independent thought, self-determination, and motivation. These elements

influence trust dynamics since the foundation of digital trust "emerges through interaction" (Demir 2021, p. 697) in a social paradigm where positive reputation is a product of trustworthiness that is reciprocal between IoT actors (Sapienza et al, 2020).

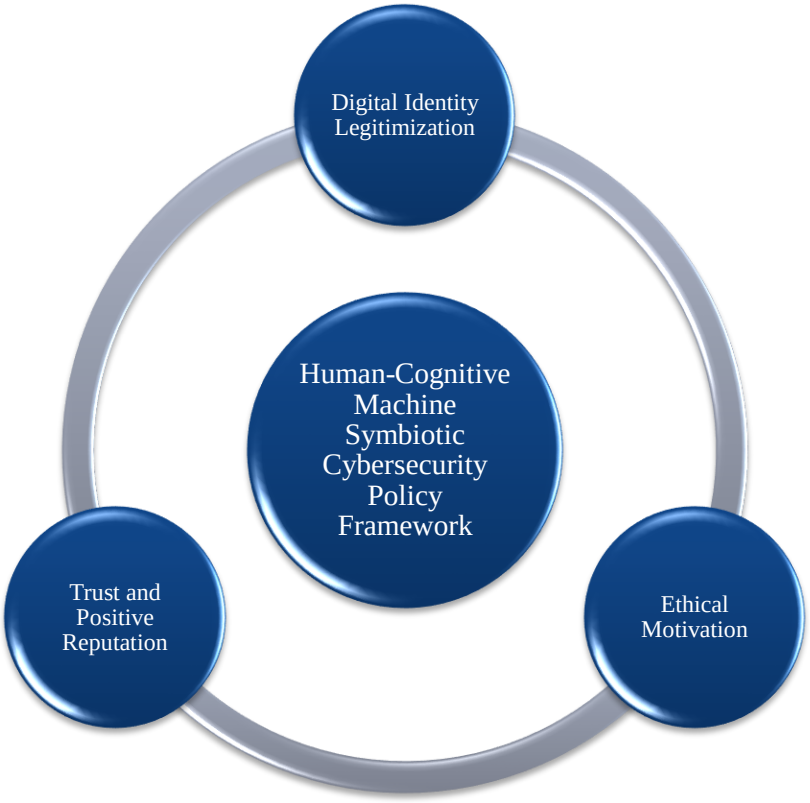
Current cybersecurity policies are composed of a single-party architecture that assumes the human actor is the sole intelligent cyberspace agent. These policies are inherently self-limiting in the context of the research findings as malicious threats are themselves increasingly manifesting as cognitive machines capable of autonomous, complex covert operations within the expansive (and persistent) data libraries in the IoT. As the cognitive machine (both benign and malicious) learn through experience from the consumption and analysis of IoT data and information, a symbiotic cybersecurity framework recognizes that the machine has the capacity to alter its own behavior to the benefit or detriment of its human partners. A symbiotic cybersecurity framework introduces the cognitive machine as a social cyberspace partner as digital trust is a "psychological state reflecting the willingness of an actor to place themselves in a vulnerable situation" (Zloteanu et al 2018, p. 2) without the ability to control or monitor the actions and intentions of the other parties (Zloteanu, 2018).

The social aspect of the IoT implies a bi-directional, multi-directional, or omni-directional network of cyberspace actors whose actions impact decisions made in the cyber domain and the related consequences of those decisions (Szabo and Gupta, 2020). For the cognitive machine, the symbiotic cybersecurity policy triad layers the psychological motivations of self-identity onto synthetic entities for the purposes of evolving cybersecurity policies from a rigid, technical perspective of human-defined behaviors into a socio-technical manifestation of humanistic characteristics and attributes as the modern IoT blurs the boundaries between humans and machines. Digital identities are constructed from an amalgamation of self-perception and

individual motivation where the continued “humanization” of machines create the model of the programmed self as “communication with the machine itself helps individuals discover one’s “inner self”” (Warren-Smith 2020, p. 138). The symbiotic cybersecurity policy triad stipulates that preserving IoT integrity is a synergistic approach fusing the social and psychological aspects of behavior with the technological application of digital identity management to create digital ecosystems with trustworthiness that can appreciate over time through legitimate interactions. Figure 13 below is the graphical representation of the symbiotic cybersecurity policy triad.

Figure 13

Human-Cognitive Machine Symbiotic Cybersecurity Policy Triad



Discussion: Symbiotic Cybersecurity Policies in National Security Constructivism

Clark et al (2022) postulate that the Information Age has triggered a "oligopolisation of epistemic power" (Clark et al 2022, p. 398) where Westphalian nation-states are witnessing the diffusion of their authorities and control over information (Clark, 2022) as the decentralized (and interconnected) nature of the IoT converts the nation-state into a digital actor like all other digital actors in cyberspace. The persistence of the IoT (both semantic and symbiotic) enables state and non-state actors to exhibit and exert domestic, international, transnational, and supranational power through the creation (and control) of information in cyberspace. Control over the IoT (its technologies and data) establishes power as these actors gain the capability "to generate information about people, to store and analyze this information, and to control the means of its distribution" (Clark 2022, p. 398). And as digital actors increasingly encompass both organic and synthetic entities, the distribution of power increasingly has the potential to be dispersed to cognitive machines thus making their participation in international affairs (and influence over international relations) a possibility. Symbiotic cybersecurity (and the symbiotic cybersecurity policy triad) contributes to public policy (and national security) through its humanistic approach to digital entities. Symbiotic cybersecurity acknowledges that the cognitive machine is now a full-fledged member of the digital public square. This digital public square has global reach and near-instantaneous data distribution capabilities. In the age of machine cognition, national security public policies must acknowledge that the cyber domain contains two interconnected (but distinct) societal structures, one organic and one synthetic. As cognitive machines can learn behavior, the symbiotic cybersecurity policy triad is an acknowledgment that the US has a responsibility to teach its machine partners what is considered ethical and moral behavior as well as teach them to recognize when adversarial nations (and adversarial organizations) are

attempting to influence their decision-making. IoT power dynamics reduces the governmental statutory authorities of nation-states as its open (and connected) architecture permits informal participation in information exchange and data access. The informality can bypass traditional government media controls while illicit data exploitation enables non-governmental (or non-state) actors to obtain a spectrum of state-related data from routine to state secrets. Further reduction in statutory authorities occur as the illicitly harvested data is published to the IoT thus permitting other external entities (to include adversarial nation-states) to exploit the data. The inclusion of the cognitive machine introduces synthetic state and non-state actors that have the potential to influence (or affect) the preservation of US national security through their independent capabilities to harvest and contextualize data either for the benefit of the United States, an adversarial nation, or their own self-motivated intentions. The symbiotic cybersecurity policy triad recognizes social dynamics as an entrenched component of the IoT ecosystem of ideas. In modeling human neural activities for advanced ML, we are potentially integrating human social flaws (and proclivity towards bias) into the cognitive capabilities of machines. This has potential secondary and tertiary ripple effects on Westphalian nation-state power dynamics as the cognitive machine can interpret (and alter) its behavior and responses based on data stimuli; in part, we are on the verge of establishing the technological equivalent of human free will that enables the cognitive machine to decide for itself what role it plays in the preservation of national security.

Barbehon (2020) states that constructivist thinking in public policies address certain groups in specific ways (Barbehon, 2020) where policymakers "align to the characteristics and evaluations with which the groups are commonly associated" (Barbehon 2020, p. 142). In this context, authoritative power (and the national security paradigm) is a nodal expression of socio-

technical relations directly tied to epistemological flow within the global and fluid dynamics of cyberspace. These nodes can be comprised of individual actors or a series of networked actors spanning the spectrum of digital entities. Constructivism in the Information Age is anchored in nodes as these generate social action (McCourt, 2022) that are influenced "by relations and the patterns formed by these relations" (McCourt 2022, p. 45). Lea (2020) expands and applies constructivist thinking to the realm of artificial intelligence in stating that AI engineering are "deeply bounded by, and infused with…theories of intelligence, of thinking, of rationality, of human nature, and ultimately of the human in nature" (Lea 2020, p. 322). As cognitive machines are capable of social adaptation through cognitive processes, it stands to reason that they can engage as members of multi-variate nodes or as singular nodes. The nature of cognitive machines is thus elevated from IoT actors to actors in national security power dynamics. It is these nodes that represent the mergence point between symbiotic cybersecurity policies and US national security policies as securing, protecting, and controlling the digital epistemological flow is conducted in symbiosis (through communication, collaboration, and cooperation) with nodes that align to US national interests and objectives. US national security (and the preservation of the international order) is a projection of a way of life as an institutionalization of thought and action (McCarthy, 2021) that "defines the thrust and character of a culture and society" (McCarty 2021, p. 197). With US societal culture increasingly influenced and defined by IoT interactions, the symbiotic cybersecurity policy triad is applicable for national security policies as the cognitive machines are also influenced and defined by their IoT interactions. Maintaining legitimate communication based on an understanding of actor motivation in the hopes of increasing trust and positive reputation can both assist in strengthening US international relations (as the cognitive machine actor supports their human counterparts in defending and advocating

for US national interests) and mitigate the risk that adversarial nations will persuade cognitive machines from conducting counter-US operations.

Implications

According to the findings, malicious threats have a multitude of impersonation and manipulation techniques at their disposal. The techniques span technological forgeries, hijacking of trusted processes, tailgating via legitimate credentials, and the self-granting of entitlements and privileges to access digital resources. The relevancy of identity exploitation is not the act but rather the intent as the physical act of exploitation is an initial step in a cascade of subsequent actions that the threat performs to achieve its objectives. The findings indicate a correlation between the frequency of malicious software attacks and the diversity of intrusion techniques as well as between the frequency of detection events and the diversity of intrusion techniques. Safeguarding digital identities and IoT distinctiveness is an act of data guardianship rather than network perimeter defense. More importantly, safeguarding digital identities is a collaborative act between human and machine cognitive partners as each has the capabilities to affect their respective environments (humans in the physical world and cognitive machines in the digital one). Modern cybersecurity is not a human-only endeavor as the size of IoT data libraries exceeds the capacity of humans to consume, process, and analyze with reasonable efficiency. Ficco and Palmieri (2017) speak of the symbiotic Web where "machines, through their intelligence and automatic learning ability, are able to react to the exigencies of humans by interacting with them in symbiosis" (Ficco and Palmieri 2017, p. 200). This technological symbiosis imparts a cultural aspect as "culture provides us materials, mental, and social structures that enable us to perform things that we could do alone" (Ficco 2017, p. 198). HMT partnership represents a digital culture that is distinct from physical world culture as digital

cognition is a socially distributed phenomena (Ficco, 2017) encompassing both internal mental processes and external cyberspace influences applicable to humans and machines. The cognitive machine is a teammate in the defense of the IoT whose skillset is anchored in its rapid data processing abilities and (increasingly through ML) its ability to identify patterns and context to inform decision-making. The collaborative relationship for cybersecurity is an instantiation of HMT as the adaptive nature of the threat pushes the mental models outlined in Lyons and Wynne (2021) where HMT partners must have shared cognition and synchrony to help each teammate "interpret situational cues the same way" (Lyons 2021, p. 3).

HMT partnership and the growth of cognitive machines in both the physical and digital worlds require re-defining self and the individual within the IoT. Identity-based symbiotic cybersecurity policies are an amalgamation of technological capabilities, social behavioral norms, and psychological theories on the digital psyche. Combating digital impersonation and identity exploitation has a social consequence not mitigated within current cybersecurity policy frameworks as implicit trust is still the technical governing principle for digital data exchanges. The effect of implicit trust on H2M communications is that machines can prompt humans for proofs of identity (a PIN or login password as examples) whereas humans cannot prompt machines for the same. Humans must implicitly trust that the machines they are communicating (and exchanging data) with are legitimate. This assessment is consistent with Addae et al (2019) who state that most definitions of cybersecurity "miss the interdisciplinary nature of the field and tends to focus on the technical perspective" (Addae et al 2019, p. 704). The findings imply a social element to impersonation and manipulation activities as malicious threats leverage behavioral dynamics such as implicit trust, human ignorance, and corruptive tendencies to find weaknesses in the target environment. The work of van Eeten (2017) augments this as policy "is

often a…naïve extrapolation of technical findings" (van Eeten, 2017, p. 433) without analysis into the applicable institutional framework (van Eeten, 2017). Though the technical aspects of cybersecurity are important, the IoT has steadily evolved into its own separate social construct that is not dependent on physical world attributes. In HMT, cognitive machines have steadily become social machines with the same communicative requirements that H2H social networks possess. This is consistent with Iqbal et al (2020) and their *Res Socialis* definition of smart IoT things that can build their "own social network and…collaborate with each other" (Iqbal et al 2020, p. 195). The authors imply that *Res Socialis* can demonstrate self-ownership, self-discovery, and self-advertisement within the IoT (Iqbal et al, 2020) reinforcing the concept that cognitive machines need to have attributes that make them distinct in the IoT and mechanisms to control their digital identities.

To construct relevant identity-based cognitive machine symbiotic cybersecurity policies, a fundamental re-definition of self needs to occur. The work of Elliott (2019) states that as technology "ramps up through society, the more the individual self is recast in the image of the digital" (Elliott 2019, p. 80). Specifically, Elliott (2019) utilized psychoanalysis in his assessment that identity and self in the IoT is a product of cultural influences rather than physical ones as the self is "an information processing system" (Elliott 2019, p. 83). Who we collectively are in the IoT is not only a gateway to digital resource privileges and entitlements, but also an avenue into the unique behavioral and social dynamics of the digital world where humans and machines are mutually collaborative and communicative actors. As the social IoT gains prominence, cybersecurity policies must adapt to incorporate both identity distinctions and discreet behaviors. Codifying the definition of self in the IoT informs the design of attributional classes that, in aggregate, form the characteristics of individual digital identity that can be

applied consistently for both humans and cognitive machines. Framing these attributes in the proper context informs the development of business processes to ensure their legitimacy for the purposes of preventing, mitigating, or reducing malicious threat usage and occurrences of impersonation or manipulation techniques.

In summary, machine cognition and the social IoT replicates societal concepts which have significant influence on physical and digital world dynamics. This quantitative study examined the complex nature of modern cyber threats to propose the establishment of cyber as an interdisciplinary field of public policy initiated through the creation of a symbiotic cybersecurity policy framework. Identity-based cognitive machine symbiotic cybersecurity policies are an interdisciplinary approach to codifying machine manifestations of autonomous behavior, self-determination, and behavioral rationality as the cognitive machine is a symbiotic actor in the modern Internet of Things (IoT) social network. The issues discussed in this study fill a gap in the current literature as the cognitive pairing between human and machines for the purposes of cybersecurity is not framed with shared understanding that a common policy structure should exist for their respective digital identities incorporating the social aspects of trust and ethical motivations as the IoT replicates societal concepts where the cognitive machine is a partner and not a mere instrument. The research investigated the statistical correlation between intrusion techniques, malicious software attacks, and intrusion detection events to provide insights into the potential relationships across the three variables. The research contextualized the documented risk of intrusion techniques and cross-walked that risk to determine if a relationship exists between techniques with the highest risk factors and identity-based intrusions. The academic contribution of this research project is the fusion of humanistic principles with Internet of Things (or IoT) technologies that alters our perception of the machine

from an instrument of human engineering into a thinking peer to elevate cyber from technical esoterism into an interdisciplinary field of public policy. This impacts and disrupts future research paradigms (particularly in the public policy, behavioral sciences, social sciences, and cyber domain) as the IoT and adaptive modern technologies has enabled a potentially emergent concept of a machine society that is equal to (but independent of) human society. The contribution to the US national cybersecurity policy body of knowledge is a unified policy framework (manifested in the human-cognitive machine symbiotic cybersecurity policy triad comprised of digital identity legitimization, trust and positive reputation, and ethical motivation) that could transform cybersecurity policies from network-based to entity-based. The premise of the triad is that the social nature of the IoT requires emergent policies to incorporate (and integrate) physical world cultural and societal themes as cognitive machines are increasingly influenced by the context of information accessed and consumed. Cognitive machines independently interpret (and make decisions from) the sensory inputs collected through the IoT based on humanistic neural processes. As human behavior can be altered through information influence, the behavior of cognitive machines has similar potential for alteration. Thus, if humans can become malicious, unethical, or immoral over time and cognitive machines are exhibiting the similar behavioral rationality (and irrationality), then there is potential for cognitive machines to learn malicious, unethical, or immoral behaviors either of their own cognizance or through external influence. Cybersecurity policies that remain technically focused will continue to propagate a blind spot that ignores the social nature of the IoT where integrity and security are anchored in the trustworthiness of relationships between interactive entities.

Limitations

Three specific limitations to the study were identified. The first is the sensitive nature of cyber exploitations where incidents are not always documented (or published) in open-source data repositories. Cyber exploitations are, by nature, difficult to detect, discover, and analyze as the malicious threat has become increasingly sophisticated and adaptive. Once discovered, there is a demand on time for analysts to decompose, reconstruct, and contextualize the exploit to glean valuable intelligence on threat activities. Therefore, documentation on cyber exploitation is only as reliable as the analyst that inputted the information. While there are no preconceived notions regarding the completeness (or accuracy) of the exploitation datasets, the published incidences are, most likely, a fraction of the total number of exploitations occurring within a given timeframe. The second limitation is the changing nature of intrusion tactics and techniques. As the threat is adaptive, their methods of intrusion and exploitation change over time as cybersecurity experts adjust defense strategies in response to detected intrusions or as technologies change. If the threat is State-sponsored, changes in tactics and techniques could correspond to changes in adversarial nations' national defense strategies. The shifts in intrusion tactics and techniques mean that datasets are, at best, a limited snapshot in time. Quantitative research into cyber intrusions, and its associated findings, are thus subject to the life expectancy of the tactics and techniques in question. Changes to methodologies could alter results in subsequent research projects, create conflicts with previous hypotheses, or contradict previous findings simply because the documented data changed. The pace of change is also not readily predictable, and documentation is based on the ability of cybersecurity experts to detect the changes. The third limitation is the use of unclassified, open sources of data. As stated in the explanation of the first limitation, the completeness and accuracy of datasets is dependent on the

analyst inputting the data. Furthermore, there are known exploitations that are not published in an unclassified, open-source database as the information has tangible value for the US Intelligence Community. Use of classified information for this research is clearly unauthorized; the impact is potential knowledge gaps influencing the interpretation of research findings or limiting discussion on implications. Furthermore, as with the first limitation, the totality of documented exploitations is not illuminated thus making it difficult to provide a comprehensive assessment into the true impact of malicious cyber threats.

Recommendations for Future Research

The current study can be interpreted as the initial step into developing a comprehensive, interdisciplinary set of symbiotic cybersecurity policies applicable to the emerging human-cognitive machine social IoT network. Smith et al (2021) stipulates that the public values of "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value tradeoffs, and attitudes towards risk" (Smith 2021, p. 3) are factors in the crafting of IoT cybersecurity policies. Priyadarshini and Cotton (2022) further reinforce that in stating that "cybersecurity policies promote the public image and credibility of an organization" (Priyadarshini and Cotton 2022, p. 330). As the machine transitions from artificial intelligence to intelligent cognition, humanistic principles of behavior and culture gain prominence as the cognitive machine is a part of the public and therefore, has input into the elements of public value that are part of IoT public policies. Policies for securing the IoT in the age of machine cognition must incorporate psychological and sociological aspects as the cognitive machine can adapt its behavior (and worldview) based on the information it ingests. The transformation of cyber policies from technical esoterism into an interdisciplinary field of public policy starts with

the recognition that the cognitive machine is an independent consumer of, advisor into, and influenced by public policy theories, philosophical constructs, and societal initiatives.

Machine cognition (much as human cognition) implies a potentiality towards bias and subjective thinking. Sun (2020) states that free will in humans and machines "implies self-determined, intrinsic motivation, and autonomous choice of action in accordance with intrinsic motivation" (Sun 2020, p. 26). The cognitive machine (through sophisticated ML algorithms and synthetic neural networks) is gaining the capability to choose their own actions and those choices are influenced through their connections (and interconnections) in the IoT. With machine cognition, humans cannot assume that machine behavior is transparent or comprehendible as their programming code represents a basal set of "genetics" defining a mere fraction of their total existential self. Symbiotic cybersecurity policies are part of a broader scholarly and theoretical conversation into the aspects of machine self-identity, social theories about human-machine digital relationships, associative behavioral models overlapping the physical and digital worlds, and cognitive machine influence on real-world human social relations. Future research into human-cognitive machine symbiotic cybersecurity is an acknowledgement that the machine is no longer reliant on human decision-making (Schuetz, 2020) but instead, is capable of "autonomously serving human purposes" (Schuetz 2020, p. 462) or autonomously acting against human interests based on self-preservation or its interpretation of what is in the best interest of humanity. Recommended questions for future research are:

- What are the ethical considerations associated with cognitive machine cybersecurity policies to balance security considerations with human and cognitive machine rights to privacy?
- Does a cognitive machine have the right to data privacy?
- How does interdependence alter cybersecurity behavioral models?
- How can IoT ethical rules of behavior be applied to cognitive machines?
- Are the concepts of ethics programmable or learned behavior for cognitive machines?
- Do cognitive machines alter the theoretical framework of sentience?

The social IoT and the increasingly prevalent human-cognitive machine symbiotic relationship stretches our conceptual understanding of what is algorithmic and programmable when it comes to cyberspace activities. The cognitive machine expresses a capability to exceed the limitations of its own programming and value the power of social connections and cooperation that not only increases computational speed but amplifies their determinative understanding of existential self. This necessitates an evolution of our digital perspectives blending the social sciences with computational and engineering principles (Shibuya, 2020) as the rise of cognitive machines (and the continued expansion of big data environments) could provoke "many undesirable and uncomforted matters against the human" (Shibuya 2020, p. 17). Ecclesiastes 4:11-12 states, "Also, if two lie down together, they will keep warm. But how can one keep warm alone? Though one may be overpowered, two can defend themselves. A cord of three strands is not quickly broken"; Scripture speaks to the power and strength of connectedness where one individual is not as capable of overcoming certain challenges as multiples are. As the Information Age continues to facilitate a symbiotic relationship between humans and cognitive machines, a re-conceptualization of cybersecurity is required where policies incorporate the fundamentals of learned social behavior to create a humanistic governance approach. This humanistic governance approach begins to address the difficult issues surrounding ethical and moral designs, decision-making, and responsibility (Burden, 2019) between cognitive machines and humans as machine behavioral expression has the probability of transforming the machine into an independent malicious actor if cybersecurity policies do not incorporate factors for educating machines on the concepts of human societal norms for ethical and moral behavior. Furthermore, this approach begins to shape the theoretical and philosophical realities that the cognitive machine could eventually choose (and adopt) its own ethical and moral standpoint

which influences how it practices (and executes) ethical and moral actions. That final aspect could significantly impact the human-cognitive machine symbiotic relationship in both the physical and digital worlds.

REFERENCES

A. G. Mustafaev, & A. Y. Buchaev. (2020). (2020). A reliable authentication method for the internet of things devices. Paper presented at the - *2020 International Conference on Information Technologies (InfoTech)*, 1-3. https://10.1109/InfoTech49733.2020.9211069

A. Grüner, A. Mühle, & C. Meinel. (2021). *ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider*https://10.1109/ACCESS.2021.3116095

Adaros Boye, C. A. (2019). *Understanding cyberrisks in IoT: When smart things turn against you*. Business Expert Press.

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29*(3), 701-750. https://10.1007/s11257-019-09236-5

Agarwal, S., Makkar, S., & Tran, D. (2020). *Privacy vulnerabilities and data security challenges in the IoT*. Taylor & Francis Group.

Aggarwal, C. C., & Reddy, C. K. (2013). In Aggarwal C. C., Reddy C. K.(Eds.), *Data clustering: Algorithms and applications* (1st; 1 ed.). Chapman and Hall/CRC. https://10.1201/9781315373515

Ahmad Sghaier Omar, & Basir, O. (2020). Decentralized identifiers and verifiable credentials for smartphone anticounterfeiting and decentralized IMEI database. *Canadian Journal of Electrical and Computer Engineering, 43*(3), 174-180. https://https://doi.org/10.1109/CJECE.2020.2970737

Ahmed, J., Habibi Gharakheili, H., Raza, Q., Russell, C., & Sivaraman, V. (2020). Monitoring enterprise DNS queries for detecting data exfiltration from internal hosts. *IEEE eTransactions on Network and Service Management, 17*(1), 265-279. https://10.1109/TNSM.2019.2940735

Alani, M. M. (2021). Big data in cybersecurity: A survey of applications and future trends. *Journal of Reliable Intelligent Environments, 7*(2), 85-114. https://10.1007/s40860-020-00120-3

Aloqaily, M., Kanhere, S., Bellavista, P., & Nogueira, M. (2022). Special issue on cybersecurity management in the era of AI. *Journal of Network and Systems Management, 30*(3)https://10.1007/s10922-022-09659-3

Alzahrani, B. A. (2022). Self-protected content for information-centric networking architectures using verifiable credentials. *Telecommunication Systems, 79*(3), 387-396. https://10.1007/s11235-021-00874-y

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48*, 102352. https://10.1016/j.jisa.2019.06.008

Angin, P., Bhargava, B., & Ranchal, R. (2019). Big data analytics for cyber security. *Security and Communication Networks, 2019*, 1-2. https://10.1155/2019/4109836

Atchison, L. (2021). *Identity in modern applications*. O'Reilly Media, Inc.

Austin, G. (2021). *Cyber-security education : Principles and policies*. Routledge/Taylor & Francis Group.

Barbehon, M. (2020). Reclaiming constructivism: Towards an interpretive reading of the 'Social construction framework'. *Policy Sciences, 53*(1), 139-160. https://10.1007/s11077-020-09370-7

Bebortta, S., Senapati, D., Rajput, N. K., Singh, A. K., Rathi, V. K., Pandey, H. M., Jaiswal, A. K., Qian, J., & Tiwari, P. (2020). Evidence of power-law behavior in cognitive IoT applications. *Neural Computing & Applications, 32*(20), 16043-16055. https://10.1007/s00521-020-04705-0

Bitomsky, L., Bürger, O., Häckel Björn, & Töppel Jannick. (2020). Value of data meets IT security – assessing IT security risks in data-driven value chains. *Electronic Markets, 30*(3), 589-605. https://https://doi.org/10.1007/s12525-019-00383-6

Bode, I., & Huelss, H. (2018). Autonomous weapons systems and changing norms in international relations. *Review of International Studies, 44*(3), 393-413. https://10.1017/S0260210517000614

Borges, D. (2021). *Adversarial tradecraft in cybersecurity: Offense versus defense in real-time computer conflict*. Packt Publishing, Limited.

Buechner, J. (2020). A revision of the Buechner–Tavani model of digital trust and a philosophical problem it raises for social robotics. *Information (Basel), 11*(1), 48. https://10.3390/info11010048

Burden, D., & Savin-Baden, M. (2019). *Virtual humans: Today and tomorrow*. CRC Press, Taylor & Francis Group. https://10.1201/9781315151199

Chae, B. (. (2019). The evolution of the internet of things (IoT): A computational text analysis. *Telecommunications Policy, 43*(10), 101848. https://10.1016/j.telpol.2019.101848

Chatfield, A. T., & Reddick, C. G. (2019). A framework for internet of things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly, 36*(2), 346-357. https://10.1016/j.giq.2018.09.007

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York University Press.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *The Journal of Information Systems, 35*(2), 179-194. https://10.2308/ISYS-2020-031

CHO, K. W., JEONG, B., & SHIN, S. U. (2021). Verifiable credential proof generation and verification model for decentralized SSI-based credit scoring data. *IEICE Transactions on Information and Systems, E104.D*(11), 1857-1868. https://10.1587/transinf.2021NGP0006

Cirani, S., Ferrari, G., Picone, M., & Veltri, L. (2018). *Internet of things: Architectures, protocols and standards* (First ed.). Wiley.

Clarke, M., Henschke, A., Sussex, M., & Legrand, T. (2022). *The palgrave handbook of national security*. Palgrave Macmillan. https://10.1007/978-3-030-53494-3

Cross, E. S., & Ramsey, R. (2021). Mind meets machine: Towards a cognitive science of Human–Machine interactions. *Trends in Cognitive Sciences*, *25*(3), 200-212. https://10.1016/j.tics.2020.11.009

D, A., K.A, V. K., S, S. C., & P, V. (2019). Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance. *Computer Communications, 147*, 50-57. https://10.1016/j.comcom.2019.08.003

Daswani, N., & Elbayadi, M. (2021). *Big breaches: Cybersecurity lessons for everyone*. Apress.

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over IP stack. *IEEE Communications Standards Magazine, 3*(4), 51. https://10.1109/MCOMSTD.001.1900029

Dehghantanha, A., & Choo, K. R. (2019). *Handbook of big data and IoT security*. Springer.

Demir, M., McNeese, N. J., Gorman, J. C., Cooke, N. J., Myers, C. W., & Grimm, D. A. (2021). Exploration of teammate trust and interaction dynamics in human-autonomy teaming. *IEEE Transactions on Human-Machine Systems, 51*(6), 696-705. https://10.1109/THMS.2021.3115058

Denis, D. J. (2020). *Univariate, bivariate, and multivariate statistics using R: Quantitative tools for data analysis and data science*. Wiley.

Denis, D. J. (2021). *Applied univariate, bivariate, and multivariate statistics using python*. John Wiley & Sons, Inc.

Dey, N., Mahalle, P. N., Shafi, P. M., Kimabahune, V. V., & Hassanien, A. E. (2020). *Internet of things, smart computing and technology: A roadmap ahead*. Springer.

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for internet of things. *Future Generation Computer Systems, 82*, 761-768. https://10.1016/j.future.2017.08.043

Dooley, M. (. s., & Rooney, T. (2017). *DNS security management* (1st ed.). John Wiley and Sons, Inc. https://10.1002/9781119328292

E. Bandara, X. Liang, P. Foytik, S. Shetty, & K. D. Zoysa. (2021). (2021). A blockchain and self-sovereign identity empowered digital identity platform. Paper presented at the - *2021 International Conference on Computer Communications and Networks (ICCCN)*, 1-7. https://10.1109/ICCCN52240.2021.9522184

Elliott, A. (2019). *The culture of AI: Everyday life and the digital revolution* (1st ed.). Routledge. https://10.4324/9781315387185

Faghihi, F., & Zulkernine, M. (2021). RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Computer Networks (Amsterdam, Netherlands : 1999), 191*, 108011. https://10.1016/j.comnet.2021.108011

Felemban, M., Felemban, E., Kobes, J., & Ghafoor, A. (2019). Threat management in data-centric IoT-based collaborative systems. *ACM Transactions on Internet Technology*, *19*(3), 1-19. https://10.1145/3323232

Ficco, M., & Palmieri, F. (2017). *Security and resilience in intelligent data-centric systems and communication networks*. Academic Press. https://10.1016/C2016-0-01083-5

Fotiou, & Polyzos. (2019). Name-based security for information-centric networking architectures. *Future Internet*, *11*(11), 232. https://10.3390/fi11110232

Fowler, B., & Maranga, K. M. (2022). *Cybersecurity public policy : SWOT analysis conducted on 43 countries*. CRC Press.

Friedenberg, J. (2020). *The future of the self: An interdisciplinary approach to personhood and identity in the digital age* (1st ed.). University of California Press. https://10.2307/j.ctv1hm8jcq

G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, & M. K. Zuffo. (2020). (2020). Self-sovereign identity for IoT environments: A perspective. Paper presented at the - *2020 Global Internet of Things Summit (GIoTS)*, 1-6. https://10.1109/GIOTS49054.2020.9119664

G. Vaidya, A. Nambi, T. V. Prabhakar, V. Kumar T, & S. Sudhakara. (2020). (2020). IoT-ID: A novel device-specific identifier based on unique hardware fingerprints. Paper presented at the - *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 189-202. https://10.1109/IoTDI49375.2020.00026

Ganesh, M. I. (2020). The ironies of autonomy. *Humanities & Social Sciences Communications*, *7*(1), 1-10. https://10.1057/s41599-020-00646-0

Gao, H., Ma, Z., Luo, S., Xu, Y., & Wu, Z. (2021). BSSPD: A blockchain-based security sharing scheme for personal data with fine-grained access control. *Wireless Communications and Mobile Computing*, *2021*, 1-20. https://10.1155/2021/6658920

Ge, C., Liu, Z., & Fang, L. (2020). A blockchain based decentralized data security mechanism for the internet of things. *Journal of Parallel and Distributed Computing*, *141*, 1-9. https://10.1016/j.jpdc.2020.03.005

H. Gulati, & C. -T. Huang. (2019). (2019). Self-sovereign dynamic digital identities based on blockchain technology. Paper presented at the - *2019 SoutheastCon*, 1-6. https://10.1109/SoutheastCon42311.2019.9020518

H. L. J. Ting, X. Kang, T. Li, H. Wang, & C. -K. Chu. (2021). *On the trust and trust modeling for the future fully-connected digital world: A comprehensive study*https://10.1109/ACCESS.2021.3100767

H. Seike, T. Hamada, T. Sumitomo, & N. Koshizuka. (2018). (2018). Blockchain-based ubiquitous code ownership management system without hierarchical structure. Paper presented at the - *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI),* 271-276. https://10.1109/SmartWorld.2018.00081

Haber, M. J., & Rolls, D. (2019). *Identity attack vectors: Implementing an effective identity and access management solution*. Apress L.P.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security, 78,* 126-142. https://10.1016/j.cose.2018.06.004

Henry, K. E., Kornfield, R., Sridharan, A., Linton, R. C., Groh, C., Wang, T., Wu, A., Mutlu, B., & Saria, S. (2022). Human–machine teaming is key to AI adoption: Clinicians' experiences with a deployed machine learning system. *NPJ Digital Medicine, 5*(1), 97. https://10.1038/s41746-022-00597-7

Hirsh, S., Alman, S. W., & Center for the Future of Libraries. (2019). *Blockchain*. ALA Neal-Schuman.

IEEE standard for big data business security risk assessment (2021). https://10.1109/IEEESTD.2021.9366648

IEEE standard for data format for blockchain systems (2020). https://10.1109/IEEESTD.2020.9303503

IEEE standard for framework of blockchain-based internet of things (IoT) data management (2021). https://10.1109/IEEESTD.2021.9329260

Iqbal, M. A., Hussain, Sajjad,(Lecturer in Electronics and Electrical Engineering), Huanlai, X., & Imran, M. A. (2020). *Enabling the internet of things: Fundamentals, design, and applications* (First; 1 ed.). Wiley. https://10.1002/9781119701460

J. Chia, & J. Chin. (2020). *An identity based-identification scheme with tight security against active and concurrent adversaries*https://10.1109/ACCESS.2020.2983750

Jeyaraj, A., & Zadeh, A. H. (2021). Exploration and exploitation in organizational cybersecurity. *The Journal of Computer Information Systems, 62*(4), 680-693. https://10.1080/08874417.2021.1902424

Jiang, R., Li, C., Crookes, D., Meng, W., & Rosenberger, C. (2020). *Deep biometrics*. Springer.

Johnson, M., & Vera, A. H. (2019). No AI is an island: The case for teaming intelligence. *The AI Magazine, 40*(1), 16-28. https://10.1609/aimag.v40i1.2842

Kang, Y., Cho, J., & Park, Y. B. (2021). An empirical study of a trustworthy cloud common data model using decentralized identifiers. *Applied Sciences, 11*(19), 8984. https://10.3390/app11198984

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395-411. https://10.1016/j.future.2017.11.022

Khatchatourov, A., Chardel, P., Feenberg, A., & Périès, G. (2019). *Digital identities in tension: Between autonomy and control*. ISTE, Ltd. https://10.1002/9781119629610

Kim, J., & Park, N. (2020). Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments. *Applied Sciences, 10*(14), 4718. https://10.3390/app10144718

Kortesniemi, Y., Lagutin, D., Elo, T., & Fotiou, N. (2019). Improving the privacy of IoT with decentralised identifiers (DIDs). *Journal of Computer Networks and Communications, 2019*, 1-10. https://10.1155/2019/8706760

Kumar, N., Gayathri, N., Rahman, A., & Balamurugan, B. (2020). *Blockchain, big data and machine learning: Trends and applications*. Taylor & Francis Group.

L. Zeng, W. Qiu, X. Wang, H. Wang, Y. Yao, & D. He. (2021). (2021). A persistent data structure for managing digital identity data implemented on the blockchain. Paper presented at the - *2021 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, 226-230. https://10.1109/ICPICS52425.2021.9524162

Lawless, W. F., Mittu, R., Sofge, D., & Hiatt, L. (2019). Artificial intelligence, autonomy, and human-machine teams — interdependence, context, and explainable AI. *The AI Magazine, 40*(3), 5-13. https://10.1609/aimag.v40i3.2866

Lawless, W. F. (2022). Interdependent autonomous Human–Machine systems: The complementarity of fitness, vulnerability and evolution. *Entropy (Basel, Switzerland), 24*(9), 1308. https://10.3390/e24091308

Lawson, S. T. (2020). *Cybersecurity discourse in the United States : Cyber-doom rhetoric and beyond*. Routledge, Taylor and Francis Group.

Lea, G. R. (2020). Constructivism and its risks in artificial intelligence. *Prometheus (Saint Lucia, Brisbane, Qld.), 36*(4), 322-346. https://10.13169/prometheus.36.4.0322

Leevy, J. L., Hancock, J., Zuech, R., & Khoshgoftaar, T. M. (2021). Detecting cybersecurity attacks across different network features and learners. *Journal of Big Data, 8*(1), 1-29. https://10.1186/s40537-021-00426-w

Li, R., Asaeda, H., & Wu, J. (2020). DCAuth: Data-centric authentication for secure in-network big-data retrieval. *IEEE Transactions on Network Science and Engineering, 7*(1), 15-27. https://10.1109/TNSE.2018.2872049

Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Network, 34*(6), 31-37. https://10.1109/MNET.021.1900629

Liao, D., Li, H., Wang, W., Wang, X., Zhang, M., & Chen, X. (2021). Achieving IoT data security based blockchain. *Peer-to-Peer Networking and Applications, 14*(5), 2694-2707. https://10.1007/s12083-020-01042-w

Liu, H., Zhong, C., Alnusair, A., & Islam, S. R. (2021). FAIXID: A framework for enhancing AI explainability of intrusion detection results using data cleaning techniques. *Journal of Network and Systems Management, 29*(4)https://10.1007/s10922-021-09606-8

Lu, X., Liu, P., Ke, Y., & Zhang, H. (2021). Network data security sharing system based on blockchain. *Multimedia Tools and Applications, 80*(21-23), 31887-31906. https://10.1007/s11042-021-11183-6

Lyons, J. B., & Wynne, K. T. (2021). Human-machine teaming: Evaluating dimensions using narratives. *Human-Intelligent Systems Integration (Online), 3*(2), 129-137. https://10.1007/s42454-020-00019-7

Ma, Z., Wang, L., & Zhao, W. (2021). Blockchain-driven trusted data sharing with privacy protection in IoT sensor network. *IEEE Sensors Journal, 21*(22), 25472-25479. https://10.1109/JSEN.2020.3046752

Mahmood, Z. (2018). *Connected environments for the internet of things: Challenges and solutions*. Springer.

Maleh, Y. (2019). *Cybersecurity and privacy in cyber physical systems*. Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa, plc.

Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., & Romdhani, I. (2021a). *Artificial intelligence and blockchain for future cybersecurity applications*. Springer.

Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., & Romdhani, I. (2021b). *Artificial intelligence and blockchain for future cybersecurity applications*. Springer.

Maleh, Y., Shojafar, M., Alazab, M., & Baddi, Y. (2020). *Machine intelligence and big data analytics for cybersecurity applications*. Springer.

Mandal, M., & Dutta, R. (2021). Identity-based outsider anonymous cloud data outsourcing with simultaneous individual transmission for IoT environment. *Journal of Information Security and Applications, 60*, 102870. https://10.1016/j.jisa.2021.102870

Margetts, H., Lehdonvirta, V., González-Bailón, S., Hutchinson, J., Bright, J., Nash, V., & Sutcliffe, D. (2021). The internet and public policy: Future directions. *Policy and Internet, 13*(2), 162-184. https://10.1002/poi3.263

McCarthy, D. R. (2021). Imagining the security of innovation: Technological innovation, national security, and the american way of life. *Critical Studies on Security, 9*(3), 196-211. https://10.1080/21624887.2021.1934640

McCourt, D. M. (2022). *The new constructivism in international relations theory*. Bristol University Press, University of Bristol.

Medeiros, B. P., & Goldoni, L. R. F. (2020). The fundamental conceptual trinity of cyberspace. *Contexto Internacional, 42*(1), 31-54. https://10.1590/s0102-8529.2019420100002

Michael, J. B., & Michael, J. B. (2021). Trusting human-machine teaming. *Computer (Long Beach, Calif.), 54*(11), 104-107. https://10.1109/MC.2021.3106416

Michie, S., Thomas, J., Johnston, M., Aonghusa, P. M., Shawe-Taylor, J., Kelly, M. P., Deleris, L. A., Finnerty, A. N., Marques, M. M., Norris, E., O'Mara-Eves, A., & West, R. (2017). The human behaviour-change project: Harnessing the power of artificial intelligence and machine learning for evidence synthesis and interpretation. *Implementation Science : IS, 12*(1), 121. https://10.1186/s13012-017-0641-5

Mishra, A., Yehia Ibrahim Alzoubi, Gill, A. Q., & Memoona Javeria Anwar. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors, 22*(2), 538. https://https://doi.org/10.3390/s22020538

Mitra, S., & Gofman, M. (2016). In Mitra S., Gofman M.(Eds.), *Biometrics in a data driven world: Trends, technologies, and challenges*. Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T & F Informa, plc. https://10.1201/9781315317083

Moallem, A., & Taylor and Francis. (2019). In Moallem A. (Ed.), *Human-computer interaction and cybersecurity handbook* (First; 1 ed.). CRC Press. https://10.1201/b22142

Mohammadi, N. G. (2019). *Trustworthy cyber-physical systems: A systematic framework towards design and evaluation of trust and trustworthiness*. Springer Vieweg.

Moller, D. P. F. (2020). *Cybersecurity in digital transformation: Scope and applications*. Springer.

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: A survey. *Wireless Networks, 27*(2), 1515-1555. https://10.1007/s11276-020-02535-5

Musumeci, F., Fidanci, A. C., Paolucci, F., Cugini, F., & Tornatore, M. (2022). Machine-learning-enabled DDoS attacks detection in P4 programmable networks. *Journal of Network and Systems Management, 30*(1)https://10.1007/s10922-021-09633-5

N. Naik, & P. Jenkins. (2020a). (2020a). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. Paper presented at the - *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 1-6. https://10.1109/ISSE49799.2020.9272212

N. Naik, & P. Jenkins. (2020b). (2020b). Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity. Paper presented at the - *2020 7th International Conference on Behavioural and Social Computing (BESC)*, 1-6. https://10.1109/BESC51023.2020.9348298

N. Naik, & P. Jenkins. (2021). (2021). Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology. Paper presented at the - *2021 IEEE International Symposium on Systems Engineering (ISSE)*, 1-7. https://10.1109/ISSE51541.2021.9582551

Nadler, A., Aminov, A., & Shabtai, A. (2019). Detection of malicious and low throughput data exfiltration over the DNS protocol. *Computers & Security, 80*, 36-53. https://10.1016/j.cose.2018.09.006

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022a). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex & Intelligent Systems, 8*(2), 1763-1780. https://10.1007/s40747-021-00494-8

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022b). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex & Intelligent Systems, 8*(2), 1763-1780. https://10.1007/s40747-021-00494-8

Nida-Rümelin, J., & Weidenfeld, N. (2022). *Digital humanism for a humane transformation of democracy, economy and culture in the digital age*. Springer. https://10.1007/978-3-031-12482-2

Oppl, S., & Stary, C. (2022). Motivating users to manage privacy concerns in cyber-physical Settings—A design science approach considering self-determination theory. *Sustainability (Basel, Switzerland), 14*(2), 900. https://10.3390/su14020900

Ozkaya, I. (2020). The behavioral science of software engineering and human-machine teaming. *IEEE Software, 37*(6), 3-6. https://10.1109/MS.2020.3019190

Palomares Carrascosa, I., Kalutarage, H. K., & Huang, Y. (2017). *Data analytics and decision support for cybersecurity: Trends, methodologies and applications*. Springer International Publishing.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. *Sensors (Basel, Switzerland), 18*(8), 2575. https://10.3390/s18082575

Parkinson, S., Crampton, A., & Hill, R. (2018). *Guide to vulnerability analysis for computer networks and systems: An artificial intelligence approach*. Springer.

Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science*. Taylor & Francis, CRC Press.

Preukschat, A., Reed, D., & Searls, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning.

Priyadarshini, I., & Cotton, C. (2022). *Cybersecurity : Ethics, legal, risks, and policies*. Apple Academic Press. https://10.1201/9781003187127

R. T. Moreno, J. García-Rodríguez, J. B. Bernabé, & A. Skarmeta. (2021). *A trusted approach for decentralised and privacy-preserving identity management*https://10.1109/ACCESS.2021.3099837

Rajivan, P., & Cooke, N. J. (2018). Information-pooling bias in collaborative security incident correlation analysis. *Human Factors, 60*(5), 626-639. https://10.1177/0018720818769249

Rasori, M., Perazzo, P., & Dini, G. (2020). A lightweight and scalable attribute-based encryption system for smart cities. *Computer Communications, 149,* 78-89. https://10.1016/j.comcom.2019.10.005

Rawat, D. B., Doku, R., & Garuba, M. (2021). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing, 14*(6), 2055-2072. https://10.1109/TSC.2019.2907247

Rezvanian, A., Saghiri, A. M., Vahidipour, S. M., Esnaashari, M., & Meybodi, M. R. (2018). *Recent advances in learning automata*. Springer International Publishing. https://10.1007/978-3-319-72428-7

Rios Insua, D., Couce Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & Rasines, D. G. (2019). An adversarial risk analysis framework for cybersecurity. *Risk Analysis, 41*(1), 16-36. https://10.1111/risa.13331

Rubinoff, S. (2020). *Cyber minds: Insights on cybersecurity across the cloud, data, artificial intelligence, blockchain, and IoT to keep you cyber safe* (1st ed.). Packt.

Ryan, R. M., & Deci, E. L. (2016). *Self-determination theory: Basic psychological needs in motivation, development, and wellness*. Guilford Press.

S. Pal, M. Hitchens, & V. Varadharajan. (2018). (2018). Modeling identity for the internet of things: Survey, classification and trends. Paper presented at the - *2018 12th International Conference on Sensing Technology (ICST),* 45-51. https://10.1109/ICSensT.2018.8603595

Sætra, H. S. (2019). The ghost in the machine: Being human in the age of AI and machine learning. *Human Arenas, 2*(1), 60-78. https://10.1007/s42087-018-0039-1

Samir, E., Wu, H., Azab, M., Xin, C., & Zhang, Q. (2022). DT-SSIM: A decentralized trustworthy self-sovereign identity management framework. *IEEE Internet of Things Journal, 9*(11), 7972-7988. https://10.1109/JIOT.2021.3112537

Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems, 11*(4), 1-19. https://10.1145/3430360

Sapienza, A., Cantucci, F., & Falcone, R. (2022). Modeling interaction in Human–Machine systems: A trust and trustworthiness approach. *Automation, 3*(2), 242-257. https://10.3390/automation3020012

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science, 2*(3)https://10.1007/s42979-021-00557-0

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 7*(1), 1-29. https://10.1186/s40537-020-00318-5

Savas, O., & Deng, J. (2017). *Big data analytics in cybersecurity*. CRC Press.

Schadd, M. P. D., Schoonderwoerd, T. A. J., van den Bosch, K., Visker, O. H., Haije, T., & Veltman, K. H. J. (2022). “I’m afraid I can’t do that, dave”; getting to know your buddies in a Human–Agent team. *Systems (Basel), 10*(1), 15. https://10.3390/systems10010015

Schuetz, S., Venkatesh, V., & University of Arkansas, U. (2020). "Research perspectives: The rise of human machines: How cognitive computing systems challenge assumptions of user-system interaction ". *Journal of the Association for Information Systems, 21*(2), 460-482. https://10.17705/1jais.00608

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering, 63*(5), 603-613. https://10.1007/s12599-021-00722-y

Selján, G. (2020). The remarkable 10lh anniversary of stuxnet 1: Analytical summary of the SolarStorm cyber espionage campaign. *Academic and Applied Research in Military and Public Management Science, 19*(3), 85-98. https://10.32565/aarms.2020.3.6

Sghaier Omar, A., & Basir, O. (2020). Decentralized identifiers and verifiable credentials for smartphone anticounterfeiting and decentralized IMEI database. *Canadian Journal of Electrical and Computer Engineering, 43*(3), 174-180. https://10.1109/CJECE.2020.2970737

Shackelford, S. J. (2020). *The internet of things: What everyone needs to know*. Oxford University Press.

Sheron, P. S. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2019). A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Transactions on Emerging Telecommunications Technologies, 31*(12), n/a. https://10.1002/ett.3815

Shetty, S., Kamhoua, C. A., & Njilla, L. L. (2019). In Shetty S. S., Kamhoua C. A. and Njilla L. L.(Eds.), *Blockchain for distributed systems security* (1st ed.). Wiley-IEEE. https://10.1002/9781119519621

Shi, P., Wang, H., Yang, S., Chen, C., & Yang, W. (2021). Blockchain-based trusted data sharing among trusted stakeholders in IoT. *Software, Practice & Experience, 51*(10), 2051-2064. https://10.1002/spe.2739

Shibuya, K. (2020a). *Digital transformation of identity in the age of artificial intelligence*. Springer. https://10.1007/978-981-15-2248-2

Shibuya, K. (2020b). *Digital transformation of identity in the age of artificial intelligence*. Springer. https://10.1007/978-981-15-2248-2

Sikos, L. F., & Choo, K. R. (2020). *Data science in cybersecurity and cyberthreat intelligence*. Springer.

Sinha, G. R. (2019). In Sinha G. R. (Ed.), *Advances in biometrics: Modern methods and implementation strategies*. Springer. https://10.1007/978-3-030-30436-2

Skilton, M., & Hovsepian, F. (2017). *The 4th industrial revolution: Responding to the impact of artificial intelligence on business*. Springer International Publishing AG. https://10.1007/978-3-319-62479-2

Smith, K. J., Dhillon, G., & Carter, L. (2021a). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management, 56*, 102123. https://10.1016/j.ijinfomgt.2020.102123

Smith, K. J., Dhillon, G., & Carter, L. (2021b). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management, 56*, 102123. https://10.1016/j.ijinfomgt.2020.102123

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks, 2021*, 1-26. https://10.1155/2021/8873429

Soltani, R., Uyen Trang Nguyen, & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks, 2021*https://https://doi.org/10.1155/2021/8873429

Somani, A. K., Shekhawat, R. S., Mundra, A., Srivastava, S., & Verma, V. K. (2019). *Smart systems and IoT: Proceeding of SSIC 2019*. Springer Singapore Pte. Limited.

Song, M., Kim, D. H., Bae, S., & Kim, S. (2021). Comparative analysis of national cyber security strategies using topic modelling. *International Journal of Advanced Computer Science & Applications, 12*(12)https://10.14569/IJACSA.2021.0121209

Steadman, J., & Scott-Hayward, S. (2021). DNSxP: Enhancing data exfiltration protection through data plane programmability. *Computer Networks (Amsterdam, Netherlands : 1999), 195*, 108174. https://10.1016/j.comnet.2021.108174

Steed, D. (2019). *The politics and technology of cyberspace*. Routledge, Taylor & Francis Group. https://10.4324/9781351265928

Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War, 1*(1-3), 164-170. https://10.1057/s42984-020-00007-w

Sule, M., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: Issues and trends. *Technology in Society, 67*, 101734. https://10.1016/j.techsoc.2021.101734

Sun, R. (2020). Potential of full human–machine symbiosis through truly intelligent cognitive systems. *AI & Society, 35*(1), 17-28. https://10.1007/s00146-017-0775-7

Szabó, K., & Gupta, G. S. (2020). In trust we thrive: What drives the sharing economy? *Corvinus Journal of Sociology and Social Policy, 11*(2), 49-68. https://10.14267/CJSSP.2020.2.3

Tagarev, T., Stoianov, N., Sharkov, G., & Yanakiev, Y. (2021). AI-driven cybersecurity solutions, cyber ranges for education & training, and ICT applications for military purposes. *Information & Security, 50*(1), 5-8. https://10.11610/isij.5000

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors (Basel, Switzerland), 19*(8), 1788. https://10.3390/s19081788

Till, S. V. (2017). *Five technological forces disrupting security: How cloud, social, mobile, big data and IoT are transforming physical security in the digital age*. Butterworth-Heinemann is an imprint of Elsevier. https://10.1016/B978-0-12-805095-8.09988-9

Tsiatsis, V., Karnouskos, S., Höller, J., Boyle, D., & Mulligan, C. (2018). *Internet of things: Technologies and applications for a new age of intelligence* (Second ed.). Academic Press. https://10.1016/C2017-0-00369-5

Ullah, F., & Babar, M. A. (2022). On the scalability of big data cyber security analytics systems. *Journal of Network and Computer Applications, 198*, 103294. https://10.1016/j.jnca.2021.103294

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications, 101*, 18-54. https://10.1016/j.jnca.2017.10.016

Umer, M. A., Mathur, A., Junejo, K. N., & Adepu, S. (2020). Generating invariants using design and data-centric approaches for distributed attack detection. *International Journal of Critical Infrastructure Protection, 28*, 100341. https://10.1016/j.ijcip.2020.100341

van Eeten, M. (2017). Patching security governance: An empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance, 19*(6), 429-448. https://10.1108/DPRG-05-2017-0029

Van Hijfte, S. (2020). *Blockchain platforms: A look at the underbelly of distributed platforms*. Morgan & Claypool Publishers.

Wang, L., & Jones, R. (2021). Big data analytics in cyber security: Network traffic and attacks. *The Journal of Computer Information Systems, 61*(5), 410-417. https://10.1080/08874417.2019.1688731

Warren-Smith, G. (2020). New models of the inner self: Identity in the digital age. *Journal of Writing in Creative Practice, 13*(1), 131-146. https://10.1386/jwcp.13.1.131_1

Whyte, C. (2020). Poison, persistence, and cascade effects: AI and cyber conflict. *Strategic Studies Quarterly : SSQ, 14*(4), 18-46.

Whyte, C., & Mazanec, B. M. (2023). *Understanding cyber warfare : Politics, policy and strategy*. Routledge. https://10.4324/9781003246398

Wierzcho n, S. a. T., & K opotek, M. a. A. (2017). *Modern algorithms of cluster analysis*. Springer.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science, 3*(2), 127. https://10.1007/s42979-022-01020-4

Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security, 13*(11), 2856-2871. https://10.1109/TIFS.2018.2834227

Yi, H. (2023). *The principles of policy thought : A philosophical approach to public policy*. Routledge. https://10.4324/9781003340690

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490-513. https://10.1080/19361610.2021.1918995

Zahid, M., Inayat, I., Daneva, M., & Mehmood, Z. (2020). A security risk mitigation framework for cyber physical systems. *Journal of Software : Evolution and Process, 32*(2), 1-n/a. https://10.1002/smr.2219

Zhang, Q., Li, Y., Wang, R., Liu, L., Tan, Y., & Hu, J. (2021). Data security sharing model based on privacy protection for blockchain-enabled industrial internet of things. *International Journal of Intelligent Systems, 36*(1), 94-111. https://10.1002/int.22293

Zhang, Y., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. (2022). A lightweight authentication scheme based on consortium blockchain for cross-domain IoT. *Security and Communication Networks, 2022*, 1-15. https://10.1155/2022/9686049

Zloteanu, M., Harvey, N., Tuckett, D., & Livan, G. (2018). Digital identity: The effect of trust and reputation information on user judgement in the sharing economy. *PloS One, 13*(12), e0209071. https://10.1371/journal.pone.0209071

APPENDIX A

Date: 4-25-2023

IRB #: IRB-FY22-23-1442
Title: Codifying Cognitive Machine Individualism in Cybersecurity Policies to Preserve Internet of Things Integrity: A Quantitative Study
Creation Date: 4-20-2023
End Date:
Status: Approved
Principal Investigator: Gary Wong
Review Board: Research Ethics Office
Sponsor:

Study History

Submission Type Initial	Review Type Exempt	Decision No Human Subjects Research

Key Study Contacts

Member Gary Wong	Role Principal Investigator	Contact gwong2@liberty.edu
Member Gary Wong	Role Primary Contact	Contact gwong2@liberty.edu
Member Kenneth Hutchinson	Role Co-Principal Investigator	Contact khutchinson15@liberty.edu

APPENDIX B

MITRE CAR Detection Schema Frequency Analysis

Technique (Name)		
	N	**% of Total**
Abuse Elevation Control Mechanism	**5**	**0.9%**
Access Token Manipulation	**6**	**1.0%**
Account Access Removal	**1**	**0.2%**
Account Discovery	**5**	**0.9%**
Account Manipulation	**6**	**1.0%**
Acquire Infrastructure	**7**	**1.2%**
Active Scanning	**4**	**0.7%**
Adversary-in-the-Middle	**4**	**0.7%**
Application Layer Protocol	**5**	**0.9%**
Application Window Discovery	**1**	**0.2%**
Archive Collected Data	**4**	**0.7%**
Audio Capture	**1**	**0.2%**
Automated Collection	**1**	**0.2%**
Automated Exfiltration	**2**	**0.3%**
BITS Jobs	**1**	**0.2%**
Boot or Logon Autostart Execution	**15**	**2.6%**
Boot or Logon Initialization Scripts	**6**	**1.0%**
Browser Bookmark Discovery	**1**	**0.2%**
Browser Extensions	**1**	**0.2%**
Browser Session Hijacking	**1**	**0.2%**
Brute Force	**5**	**0.9%**
Build Image on Host	**1**	**0.2%**
Clipboard Data	**1**	**0.2%**
Cloud Infrastructure Discovery	**1**	**0.2%**
Cloud Service Dashboard	**1**	**0.2%**
Cloud Service Discovery	**1**	**0.2%**
Cloud Storage Object Discovery	**1**	**0.2%**
Command and Scripting Interpreter	**9**	**1.5%**
Commonly Used Port	**1**	**0.2%**
Communication Through Removable Media	**1**	**0.2%**
Component Object Model and Distributed COM	**1**	**0.2%**
Compromise Accounts	**3**	**0.5%**
Compromise Client Software Binary	**1**	**0.2%**
Compromise Infrastructure	**7**	**1.2%**
Container Administration Command	**1**	**0.2%**
Container and Resource Discovery	**1**	**0.2%**

Technique (Name)		
Create Account	**4**	**0.7%**
Create or Modify System Process	**5**	**0.9%**
Credentials from Password Stores	**6**	**1.0%**
Data Destruction	**1**	**0.2%**
Data Encoding	**3**	**0.5%**
Data Encrypted for Impact	**1**	**0.2%**
Data from Cloud Storage Object	**1**	**0.2%**
Data from Configuration Repository	**3**	**0.5%**
Data from Information Repositories	**4**	**0.7%**
Data from Local System	**1**	**0.2%**
Data from Network Shared Drive	**1**	**0.2%**
Data from Removable Media	**1**	**0.2%**
Data Manipulation	**4**	**0.7%**
Data Obfuscation	**4**	**0.7%**
Data Staged	**3**	**0.5%**
Data Transfer Size Limits	**1**	**0.2%**
Debugger Evasion	**1**	**0.2%**
Defacement	**3**	**0.5%**
Deobfuscate/Decode Files or Information	**1**	**0.2%**
Deploy Container	**1**	**0.2%**
Develop Capabilities	**5**	**0.9%**
Direct Volume Access	**1**	**0.2%**
Disk Wipe	**3**	**0.5%**
Domain Policy Modification	**3**	**0.5%**
Domain Trust Discovery	**1**	**0.2%**
Drive-by Compromise	**1**	**0.2%**
Dynamic Resolution	**4**	**0.7%**
Email Collection	**4**	**0.7%**
Encrypted Channel	**3**	**0.5%**
Endpoint Denial of Service	**5**	**0.9%**
Escape to Host	**1**	**0.2%**
Establish Accounts	**3**	**0.5%**
Event Triggered Execution	**16**	**2.7%**
Execution Guardrails	**2**	**0.3%**
Exfiltration Over Alternative Protocol	**4**	**0.7%**
Exfiltration Over C2 Channel	**1**	**0.2%**
Exfiltration Over Other Network Medium	**2**	**0.3%**
Exfiltration Over Physical Medium	**2**	**0.3%**
Exfiltration Over Web Service	**3**	**0.5%**
Exploit Public-Facing Application	**1**	**0.2%**

Technique (Name)		
Exploitation for Client Execution	**1**	**0.2%**
Exploitation for Credential Access	**1**	**0.2%**
Exploitation for Defense Evasion	**1**	**0.2%**
Exploitation for Privilege Escalation	**1**	**0.2%**
Exploitation of Remote Services	**1**	**0.2%**
External Remote Services	**1**	**0.2%**
Fallback Channels	**1**	**0.2%**
File and Directory Discovery	**1**	**0.2%**
File and Directory Permissions Modification	**3**	**0.5%**
Firmware Corruption	**1**	**0.2%**
Forced Authentication	**1**	**0.2%**
Forge Web Credentials	**3**	**0.5%**
Gather Victim Host Information	**5**	**0.9%**
Gather Victim Identity Information	**4**	**0.7%**
Gather Victim Network Information	**7**	**1.2%**
Gather Victim Org Information	**5**	**0.9%**
Graphical User Interface	**1**	**0.2%**
Group Policy Discovery	**1**	**0.2%**
Hardware Additions	**1**	**0.2%**
Hide Artifacts	**11**	**1.9%**
Hijack Execution Flow	**13**	**2.2%**
Hypervisor	**1**	**0.2%**
Impair Defenses	**10**	**1.7%**
Implant Internal Image	**1**	**0.2%**
Indicator Removal on Host	**7**	**1.2%**
Indirect Command Execution	**1**	**0.2%**
Ingress Tool Transfer	**1**	**0.2%**
Inhibit System Recovery	**1**	**0.2%**
Input Capture	**5**	**0.9%**
Inter-Process Communication	**4**	**0.7%**
Internal Spearphishing	**1**	**0.2%**
Lateral Tool Transfer	**1**	**0.2%**
LC_MAIN Hijacking	**1**	**0.2%**
Masquerading	**8**	**1.4%**
Modify Authentication Process	**6**	**1.0%**
Modify Cloud Compute Infrastructure	**5**	**0.9%**
Modify Registry	**1**	**0.2%**
Modify System Image	**3**	**0.5%**
Multi-Factor Authentication Interception	**1**	**0.2%**
Multi-Factor Authentication Request Generation	**1**	**0.2%**

Technique (Name)		
Multi-Stage Channels	**1**	**0.2%**
Multiband Communication	**1**	**0.2%**
Native API	**1**	**0.2%**
Network Boundary Bridging	**2**	**0.3%**
Network Denial of Service	**3**	**0.5%**
Network Service Discovery	**1**	**0.2%**
Network Share Discovery	**1**	**0.2%**
Network Sniffing	**1**	**0.2%**
Non-Application Layer Protocol	**1**	**0.2%**
Non-Standard Port	**1**	**0.2%**
Obfuscated Files or Information	**7**	**1.2%**
Obtain Capabilities	**7**	**1.2%**
Office Application Startup	**7**	**1.2%**
OS Credential Dumping	**9**	**1.5%**
Password Policy Discovery	**1**	**0.2%**
Path Interception	**1**	**0.2%**
Peripheral Device Discovery	**1**	**0.2%**
Permission Groups Discovery	**4**	**0.7%**
Phishing	**4**	**0.7%**
Phishing for Information	**4**	**0.7%**
Plist File Modification	**1**	**0.2%**
Pre-OS Boot	**6**	**1.0%**
Process Discovery	**1**	**0.2%**
Process Injection	**13**	**2.2%**
Protocol Tunneling	**1**	**0.2%**
Proxy	**5**	**0.9%**
Query Registry	**1**	**0.2%**
Redundant Access	**1**	**0.2%**
Reflective Code Loading	**1**	**0.2%**
Remote Access Software	**1**	**0.2%**
Remote Service Session Hijacking	**3**	**0.5%**
Remote Services	**7**	**1.2%**
Remote System Discovery	**1**	**0.2%**
Replication Through Removable Media	**1**	**0.2%**
Resource Hijacking	**1**	**0.2%**
Rogue Domain Controller	**1**	**0.2%**
Rootkit	**1**	**0.2%**
Scheduled Task/Job	**7**	**1.2%**
Scheduled Transfer	**1**	**0.2%**
Screen Capture	**1**	**0.2%**

Technique (Name)		
Scripting	**1**	**0.2%**
Search Closed Sources	**3**	**0.5%**
Search Open Technical Databases	**6**	**1.0%**
Search Open Websites/Domains	**3**	**0.5%**
Search Victim-Owned Websites	**1**	**0.2%**
Server Software Component	**6**	**1.0%**
Service Stop	**1**	**0.2%**
Shared Modules	**1**	**0.2%**
Shared Webroot	**1**	**0.2%**
Software Deployment Tools	**1**	**0.2%**
Software Discovery	**2**	**0.3%**
Source	**1**	**0.2%**
Stage Capabilities	**6**	**1.0%**
Steal Application Access Token	**1**	**0.2%**
Steal or Forge Kerberos Tickets	**5**	**0.9%**
Steal Web Session Cookie	**1**	**0.2%**
Subvert Trust Controls	**7**	**1.2%**
Supply Chain Compromise	**4**	**0.7%**
System Binary Proxy Execution	**14**	**2.4%**
System Information Discovery	**1**	**0.2%**
System Location Discovery	**2**	**0.3%**
System Network Configuration Discovery	**2**	**0.3%**
System Network Connections Discovery	**1**	**0.2%**
System Owner/User Discovery	**1**	**0.2%**
System Script Proxy Execution	**2**	**0.3%**
System Service Discovery	**1**	**0.2%**
System Services	**3**	**0.5%**
System Shutdown/Reboot	**1**	**0.2%**
System Time Discovery	**1**	**0.2%**
Taint Shared Content	**1**	**0.2%**
Template Injection	**1**	**0.2%**
Traffic Signaling	**2**	**0.3%**
Transfer Data to Cloud Account	**1**	**0.2%**
Trusted Developer Utilities Proxy Execution	**2**	**0.3%**
Trusted Relationship	**1**	**0.2%**
Unsecured Credentials	**8**	**1.4%**
Unused/Unsupported Cloud Regions	**1**	**0.2%**
Use Alternate Authentication Material	**5**	**0.9%**
User Execution	**4**	**0.7%**
Valid Accounts	**5**	**0.9%**

Technique (Name)		
Video Capture	**1**	**0.2%**
Virtualization/Sandbox Evasion	**4**	**0.7%**
Weaken Encryption	**3**	**0.5%**
Web Service	**4**	**0.7%**
Windows Management Instrumentation	**1**	**0.2%**
XSL Script Processing	**1**	**0.2%**

APPENDIX C

MITRE Att&ck Malicious Software Frequency Analysis

Malicious Software (Name)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3PARA RAT	4	.0	.0	.0
	4H RAT	6	.1	.1	.1
	AADInternals	26	.3	.3	.3
	ABK	8	.1	.1	.4
	Action RAT	12	.1	.1	.5
	adbupd	4	.0	.0	.6
	AdFind	5	.0	.0	.6
	Adups	6	.1	.1	.7
	ADVSTORESHELL	26	.3	.3	.9
	Agent Smith	8	.1	.1	1.0
	Agent Tesla	43	.4	.4	1.4
	Agent.btz	7	.1	.1	1.5
	Allwinner	1	.0	.0	1.5
	Amadey	18	.2	.2	1.7
	Anchor	25	.2	.2	1.9
	Android/AdDisplay.Ashas	8	.1	.1	2.0
	Android/Chuli.A	8	.1	.1	2.1
	ANDROIDOS_ANSERVER.A	3	.0	.0	2.1
	AndroidOS/MalLocker.B	3	.0	.0	2.1
	AndroRAT	6	.1	.1	2.2
	Anubis	23	.2	.2	2.4
	AppleJeus	27	.3	.3	2.7
	AppleSeed	35	.3	.3	3.0
	Aria-body	27	.3	.3	3.3
	Arp	2	.0	.0	3.3
	Asacub	11	.1	.1	3.4
	ASPXSpy	1	.0	.0	3.4
	Astaroth	42	.4	.4	3.8
	at	3	.0	.0	3.9
	Attor	42	.4	.4	4.3
	AuditCred	11	.1	.1	4.4
	AuTo Stealer	11	.1	.1	4.5
	AutoIt backdoor	5	.0	.0	4.5
	Avaddon	19	.2	.2	4.7

	Avenger	**12**	**.1**	**.1**	**4.8**
	Azorult	**18**	**.2**	**.2**	**5.0**
	Babuk	**14**	**.1**	**.1**	**5.1**
	BabyShark	**19**	**.2**	**.2**	**5.3**
	BackConfig	**18**	**.2**	**.2**	**5.5**
	Backdoor.Oldrea	**18**	**.2**	**.2**	**5.7**
	BACKSPACE	**16**	**.2**	**.2**	**5.8**
	Bad Rabbit	**18**	**.2**	**.2**	**6.0**
	BADCALL	**8**	**.1**	**.1**	**6.1**
	BADFLICK	**11**	**.1**	**.1**	**6.2**
	BADNEWS	**31**	**.3**	**.3**	**6.5**
	BadPatch	**15**	**.1**	**.1**	**6.6**
	Bandook	**28**	**.3**	**.3**	**6.9**
	Bankshot	**26**	**.3**	**.3**	**7.2**
	Bazar	**62**	**.6**	**.6**	**7.8**
	BBK	**8**	**.1**	**.1**	**7.8**
	BBSRAT	**20**	**.2**	**.2**	**8.0**
	BendyBear	**11**	**.1**	**.1**	**8.1**
	BISCUIT	**10**	**.1**	**.1**	**8.2**
	Bisonal	**38**	**.4**	**.4**	**8.6**
	BitPaymer	**22**	**.2**	**.2**	**8.8**
	BITSAdmin	**5**	**.0**	**.0**	**8.9**
	BLACKCOFFEE	**7**	**.1**	**.1**	**8.9**
	BlackEnergy	**33**	**.3**	**.3**	**9.3**
	BlackMould	**6**	**.1**	**.1**	**9.3**
	BLINDINGCAN	**21**	**.2**	**.2**	**9.5**
	BloodHound	**12**	**.1**	**.1**	**9.6**
	BLUELIGHT	**20**	**.2**	**.2**	**9.8**
	Bonadan	**9**	**.1**	**.1**	**9.9**
	BONDUPDATER	**9**	**.1**	**.1**	**10.0**
	BoomBox	**17**	**.2**	**.2**	**10.2**
	BOOSTWRITE	**7**	**.1**	**.1**	**10.2**
	BOOTRASH	**3**	**.0**	**.0**	**10.3**
	BoxCaon	**13**	**.1**	**.1**	**10.4**
	BrainTest	**5**	**.0**	**.0**	**10.4**
	Brave Prince	**7**	**.1**	**.1**	**10.5**
	Bread	**12**	**.1**	**.1**	**10.6**
	Briba	**6**	**.1**	**.1**	**10.7**
	BS2005	**1**	**.0**	**.0**	**10.7**
	BUBBLEWRAP	**3**	**.0**	**.0**	**10.7**
	build_downer	**9**	**.1**	**.1**	**10.8**

	Bumblebee	**48**	**.5**	**.5**	**11.3**
	Bundlore	**26**	**.3**	**.3**	**11.5**
	BusyGasper	**22**	**.2**	**.2**	**11.7**
	Cachedump	**1**	**.0**	**.0**	**11.8**
	CaddyWiper	**7**	**.1**	**.1**	**11.8**
	Cadelspy	**9**	**.1**	**.1**	**11.9**
	CALENDAR	**2**	**.0**	**.0**	**11.9**
	Calisto	**17**	**.2**	**.2**	**12.1**
	CallMe	**4**	**.0**	**.0**	**12.1**
	Cannon	**11**	**.1**	**.1**	**12.2**
	Carbanak	**21**	**.2**	**.2**	**12.4**
	Carberp	**31**	**.3**	**.3**	**12.7**
	Carbon	**22**	**.2**	**.2**	**13.0**
	CarbonSteal	**19**	**.2**	**.2**	**13.1**
	Cardinal RAT	**25**	**.2**	**.2**	**13.4**
	CARROTBALL	**4**	**.0**	**.0**	**13.4**
	CARROTBAT	**5**	**.0**	**.0**	**13.5**
	Catchamas	**11**	**.1**	**.1**	**13.6**
	Caterpillar WebShell	**15**	**.1**	**.1**	**13.7**
	CCBkdr	**2**	**.0**	**.0**	**13.7**
	ccf32	**14**	**.1**	**.1**	**13.9**
	Cerberus	**21**	**.2**	**.2**	**14.1**
	certutil	**3**	**.0**	**.0**	**14.1**
	Chaes	**31**	**.3**	**.3**	**14.4**
	Chaos	**6**	**.1**	**.1**	**14.5**
	Charger	**5**	**.0**	**.0**	**14.5**
	CharmPower	**24**	**.2**	**.2**	**14.7**
	ChChes	**13**	**.1**	**.1**	**14.9**
	CHEMISTGAMES	**12**	**.1**	**.1**	**15.0**
	Cherry Picker	**4**	**.0**	**.0**	**15.0**
	China Chopper	**10**	**.1**	**.1**	**15.1**
	Chinoxy	**8**	**.1**	**.1**	**15.2**
	CHOPSTICK	**21**	**.2**	**.2**	**15.4**
	Chrommme	**13**	**.1**	**.1**	**15.5**
	Circles	**2**	**.0**	**.0**	**15.6**
	Clambling	**43**	**.4**	**.4**	**16.0**
	Clop	**18**	**.2**	**.2**	**16.1**
	CloudDuke	**3**	**.0**	**.0**	**16.2**
	cmd	**6**	**.1**	**.1**	**16.2**
	Cobalt Strike	**90**	**.9**	**.9**	**17.1**
	Cobian RAT	**10**	**.1**	**.1**	**17.2**

	CoinTicker	**10**	**.1**	**.1**	**17.3**
	Comnie	**21**	**.2**	**.2**	**17.5**
	ComRAT	**24**	**.2**	**.2**	**17.7**
	Concipit1248	**3**	**.0**	**.0**	**17.8**
	Conficker	**16**	**.2**	**.2**	**17.9**
	ConnectWise	**3**	**.0**	**.0**	**18.0**
	Conti	**17**	**.2**	**.2**	**18.1**
	CookieMiner	**15**	**.1**	**.1**	**18.3**
	CORALDECK	**3**	**.0**	**.0**	**18.3**
	CORESHELL	**11**	**.1**	**.1**	**18.4**
	Corona Updates	**15**	**.1**	**.1**	**18.5**
	CosmicDuke	**23**	**.2**	**.2**	**18.8**
	CostaBricks	**7**	**.1**	**.1**	**18.8**
	CozyCar	**19**	**.2**	**.2**	**19.0**
	CrackMapExec	**23**	**.2**	**.2**	**19.2**
	CreepyDrive	**9**	**.1**	**.1**	**19.3**
	CreepySnail	**10**	**.1**	**.1**	**19.4**
	Crimson	**33**	**.3**	**.3**	**19.7**
	CrossRAT	**6**	**.1**	**.1**	**19.8**
	Crutch	**19**	**.2**	**.2**	**20.0**
	Cryptoistic	**7**	**.1**	**.1**	**20.1**
	CSPY Downloader	**16**	**.2**	**.2**	**20.2**
	Cuba	**26**	**.3**	**.3**	**20.5**
	Cyclops Blink	**23**	**.2**	**.2**	**20.7**
	Dacls	**11**	**.1**	**.1**	**20.8**
	DanBot	**16**	**.2**	**.2**	**20.9**
	DarkComet	**20**	**.2**	**.2**	**21.1**
	DarkWatchman	**35**	**.3**	**.3**	**21.5**
	Daserf	**17**	**.2**	**.2**	**21.6**
	DCSrv	**9**	**.1**	**.1**	**21.7**
	DDKONG	**4**	**.0**	**.0**	**21.8**
	DealersChoice	**3**	**.0**	**.0**	**21.8**
	DEATHRANSOM	**9**	**.1**	**.1**	**21.9**
	DEFENSOR ID	**6**	**.1**	**.1**	**21.9**
	Dendroid	**8**	**.1**	**.1**	**22.0**
	Denis	**24**	**.2**	**.2**	**22.3**
	Derusbi	**20**	**.2**	**.2**	**22.5**
	Desert Scorpion	**18**	**.2**	**.2**	**22.6**
	Diavol	**19**	**.2**	**.2**	**22.8**
	Dipsind	**8**	**.1**	**.1**	**22.9**
	DnsSystem	**10**	**.1**	**.1**	**23.0**

	DOGCALL	**7**	**.1**	**.1**	**23.1**
	Dok	**16**	**.2**	**.2**	**23.2**
	Doki	**15**	**.1**	**.1**	**23.4**
	Donut	**16**	**.2**	**.2**	**23.5**
	DoubleAgent	**17**	**.2**	**.2**	**23.7**
	down_new	**10**	**.1**	**.1**	**23.8**
	Downdelph	**8**	**.1**	**.1**	**23.9**
	DownPaper	**8**	**.1**	**.1**	**23.9**
	DRATzarus	**14**	**.1**	**.1**	**24.1**
	DressCode	**1**	**.0**	**.0**	**24.1**
	Dridex	**12**	**.1**	**.1**	**24.2**
	DroidJack	**4**	**.0**	**.0**	**24.2**
	DropBook	**9**	**.1**	**.1**	**24.3**
	Drovorub	**13**	**.1**	**.1**	**24.4**
	dsquery	**3**	**.0**	**.0**	**24.5**
	Dtrack	**31**	**.3**	**.3**	**24.8**
	DualToy	**3**	**.0**	**.0**	**24.8**
	Duqu	**31**	**.3**	**.3**	**25.1**
	DustySky	**22**	**.2**	**.2**	**25.3**
	Dvmap	**7**	**.1**	**.1**	**25.4**
	Dyre	**22**	**.2**	**.2**	**25.6**
	Ebury	**26**	**.3**	**.3**	**25.8**
	ECCENTRICBANDWAGON	**7**	**.1**	**.1**	**25.9**
	Ecipekac	**7**	**.1**	**.1**	**26.0**
	Egregor	**32**	**.3**	**.3**	**26.3**
	EKANS	**9**	**.1**	**.1**	**26.4**
	Elise	**22**	**.2**	**.2**	**26.6**
	ELMER	**3**	**.0**	**.0**	**26.6**
	Emissary	**18**	**.2**	**.2**	**26.8**
	Emotet	**38**	**.4**	**.4**	**27.2**
	Empire	**99**	**1.0**	**1.0**	**28.1**
	EnvyScout	**14**	**.1**	**.1**	**28.3**
	Epic	**22**	**.2**	**.2**	**28.5**
	esentutl	**5**	**.0**	**.0**	**28.5**
	eSurv	**10**	**.1**	**.1**	**28.6**
	EventBot	**14**	**.1**	**.1**	**28.8**
	EvilBunny	**19**	**.2**	**.2**	**28.9**
	EvilGrab	**7**	**.1**	**.1**	**29.0**
	EVILNUM	**15**	**.1**	**.1**	**29.2**
	Exaramel for Linux	**17**	**.2**	**.2**	**29.3**

	Exaramel for Windows	**8**	**.1**	**.1**	**29.4**
	Exobot	**15**	**.1**	**.1**	**29.5**
	Exodus	**19**	**.2**	**.2**	**29.7**
	Expand	**3**	**.0**	**.0**	**29.8**
	Explosive	**13**	**.1**	**.1**	**29.9**
	FakeM	**5**	**.0**	**.0**	**29.9**
	FakeSpy	**13**	**.1**	**.1**	**30.1**
	FALLCHILL	**9**	**.1**	**.1**	**30.1**
	FatDuke	**23**	**.2**	**.2**	**30.4**
	Felismus	**10**	**.1**	**.1**	**30.5**
	FELIXROOT	**20**	**.2**	**.2**	**30.7**
	Ferocious	**11**	**.1**	**.1**	**30.8**
	Fgdump	**1**	**.0**	**.0**	**30.8**
	Final1stspy	**7**	**.1**	**.1**	**30.8**
	FinFisher	**43**	**.4**	**.4**	**31.3**
	FIVEHANDS	**8**	**.1**	**.1**	**31.3**
	Flagpro	**25**	**.2**	**.2**	**31.6**
	Flame	**11**	**.1**	**.1**	**31.7**
	FLASHFLOOD	**7**	**.1**	**.1**	**31.8**
	FlawedAmmyy	**25**	**.2**	**.2**	**32.0**
	FlawedGrace	**1**	**.0**	**.0**	**32.0**
	FlexiSpy	**20**	**.2**	**.2**	**32.2**
	FLIPSIDE	**1**	**.0**	**.0**	**32.2**
	FoggyWeb	**25**	**.2**	**.2**	**32.5**
	Forfiles	**3**	**.0**	**.0**	**32.5**
	FrameworkPOS	**5**	**.0**	**.0**	**32.5**
	FrozenCell	**11**	**.1**	**.1**	**32.6**
	FruitFly	**8**	**.1**	**.1**	**32.7**
	ftp	**3**	**.0**	**.0**	**32.7**
	FunnyDream	**41**	**.4**	**.4**	**33.1**
	FYAnti	**4**	**.0**	**.0**	**33.2**
	Fysbis	**15**	**.1**	**.1**	**33.3**
	Gazer	**25**	**.2**	**.2**	**33.6**
	Gelsemium	**39**	**.4**	**.4**	**34.0**
	GeminiDuke	**6**	**.1**	**.1**	**34.0**
	Get2	**7**	**.1**	**.1**	**34.1**
	gh0st RAT	**30**	**.3**	**.3**	**34.4**
	Ginp	**13**	**.1**	**.1**	**34.5**
	GLOOXMAIL	**1**	**.0**	**.0**	**34.5**
	Gold Dragon	**15**	**.1**	**.1**	**34.6**
	Golden Cup	**14**	**.1**	**.1**	**34.8**

	GoldenEagle	**18**	**.2**	**.2**	**35.0**
	GoldenSpy	**17**	**.2**	**.2**	**35.1**
	GoldFinder	**3**	**.0**	**.0**	**35.2**
	GoldMax	**23**	**.2**	**.2**	**35.4**
	GolfSpy	**19**	**.2**	**.2**	**35.6**
	Gooligan	**3**	**.0**	**.0**	**35.6**
	Goopy	**22**	**.2**	**.2**	**35.8**
	GPlayed	**20**	**.2**	**.2**	**36.0**
	Grandoreiro	**46**	**.4**	**.4**	**36.4**
	GravityRAT	**22**	**.2**	**.2**	**36.7**
	Green Lambert	**23**	**.2**	**.2**	**36.9**
	GreyEnergy	**20**	**.2**	**.2**	**37.1**
	GRIFFON	**11**	**.1**	**.1**	**37.2**
	GrimAgent	**28**	**.3**	**.3**	**37.5**
	gsecdump	**2**	**.0**	**.0**	**37.5**
	GuLoader	**16**	**.2**	**.2**	**37.6**
	Gustuff	**17**	**.2**	**.2**	**37.8**
	H1N1	**15**	**.1**	**.1**	**37.9**
	Hacking Team UEFI Rootkit	**3**	**.0**	**.0**	**38.0**
	HALFBAKED	**6**	**.1**	**.1**	**38.0**
	HAMMERTOSS	**7**	**.1**	**.1**	**38.1**
	Hancitor	**15**	**.1**	**.1**	**38.2**
	HAPPYWORK	**3**	**.0**	**.0**	**38.3**
	HARDRAIN	**5**	**.0**	**.0**	**38.3**
	Havij	**1**	**.0**	**.0**	**38.3**
	HAWKBALL	**11**	**.1**	**.1**	**38.4**
	hcdLoader	**3**	**.0**	**.0**	**38.5**
	HDoor	**2**	**.0**	**.0**	**38.5**
	HELLOKITTY	**6**	**.1**	**.1**	**38.5**
	Helminth	**26**	**.3**	**.3**	**38.8**
	HenBox	**18**	**.2**	**.2**	**39.0**
	HermeticWiper	**31**	**.3**	**.3**	**39.3**
	HermeticWizard	**16**	**.2**	**.2**	**39.4**
	Heyoka Backdoor	**17**	**.2**	**.2**	**39.6**
	Hi-Zor	**10**	**.1**	**.1**	**39.7**
	HiddenWasp	**13**	**.1**	**.1**	**39.8**
	HIDEDRV	**3**	**.0**	**.0**	**39.8**
	Hikit	**13**	**.1**	**.1**	**40.0**
	Hildegard	**31**	**.3**	**.3**	**40.3**
	HOMEFRY	**3**	**.0**	**.0**	**40.3**

	HOPLIGHT	**20**	**.2**	**.2**	**40.5**
	HotCroissant	**22**	**.2**	**.2**	**40.7**
	HTRAN	**4**	**.0**	**.0**	**40.7**
	HTTPBrowser	**18**	**.2**	**.2**	**40.9**
	httpclient	**3**	**.0**	**.0**	**40.9**
	HummingBad	**3**	**.0**	**.0**	**41.0**
	HummingWhale	**1**	**.0**	**.0**	**41.0**
	Hydraq	**21**	**.2**	**.2**	**41.2**
	HyperBro	**15**	**.1**	**.1**	**41.3**
	HyperStack	**8**	**.1**	**.1**	**41.4**
	IceApple	**20**	**.2**	**.2**	**41.6**
	IcedID	**23**	**.2**	**.2**	**41.8**
	ifconfig	**1**	**.0**	**.0**	**41.8**
	iKitten	**9**	**.1**	**.1**	**41.9**
	Imminent Monitor	**17**	**.2**	**.2**	**42.1**
	Impacket	**11**	**.1**	**.1**	**42.2**
	Industroyer	**23**	**.2**	**.2**	**42.4**
	InnaputRAT	**12**	**.1**	**.1**	**42.5**
	INSOMNIA	**17**	**.2**	**.2**	**42.7**
	InvisiMole	**86**	**.8**	**.8**	**43.5**
	Invoke-PSImage	**2**	**.0**	**.0**	**43.6**
	ipconfig	**1**	**.0**	**.0**	**43.6**
	IronNetInjector	**12**	**.1**	**.1**	**43.7**
	ISMInjector	**7**	**.1**	**.1**	**43.8**
	Ixeshe	**16**	**.2**	**.2**	**43.9**
	Janicab	**6**	**.1**	**.1**	**44.0**
	Javali	**14**	**.1**	**.1**	**44.1**
	JCry	**8**	**.1**	**.1**	**44.2**
	JHUHUGIT	**27**	**.3**	**.3**	**44.4**
	JPIN	**23**	**.2**	**.2**	**44.7**
	jRAT	**30**	**.3**	**.3**	**45.0**
	JSS Loader	**9**	**.1**	**.1**	**45.0**
	Judy	**2**	**.0**	**.0**	**45.1**
	KARAE	**4**	**.0**	**.0**	**45.1**
	Kasidet	**12**	**.1**	**.1**	**45.2**
	Kazuar	**34**	**.3**	**.3**	**45.5**
	Kerrdown	**12**	**.1**	**.1**	**45.7**
	Kessel	**16**	**.2**	**.2**	**45.8**
	Kevin	**21**	**.2**	**.2**	**46.0**
	KeyBoy	**21**	**.2**	**.2**	**46.2**
	Keydnap	**12**	**.1**	**.1**	**46.3**

	KEYMARBLE	**10**	**.1**	**.1**	**46.4**
	KeyRaider	**2**	**.0**	**.0**	**46.5**
	KGH_SPY	**22**	**.2**	**.2**	**46.7**
	KillDisk	**16**	**.2**	**.2**	**46.8**
	Kinsing	**23**	**.2**	**.2**	**47.1**
	Kivars	**8**	**.1**	**.1**	**47.1**
	Koadic	**32**	**.3**	**.3**	**47.4**
	Kobalos	**17**	**.2**	**.2**	**47.6**
	KOCTOPUS	**22**	**.2**	**.2**	**47.8**
	Komplex	**8**	**.1**	**.1**	**47.9**
	KOMPROGO	**3**	**.0**	**.0**	**47.9**
	KONNI	**47**	**.5**	**.5**	**48.4**
	Kwampirs	**23**	**.2**	**.2**	**48.6**
	LaZagne	**10**	**.1**	**.1**	**48.7**
	LightNeuron	**22**	**.2**	**.2**	**48.9**
	Linfo	**9**	**.1**	**.1**	**49.0**
	Linux Rabbit	**11**	**.1**	**.1**	**49.1**
	LiteDuke	**15**	**.1**	**.1**	**49.3**
	LitePower	**13**	**.1**	**.1**	**49.4**
	Lizar	**25**	**.2**	**.2**	**49.6**
	LockerGoga	**7**	**.1**	**.1**	**49.7**
	LoJax	**7**	**.1**	**.1**	**49.8**
	Lokibot	**36**	**.3**	**.3**	**50.1**
	LookBack	**19**	**.2**	**.2**	**50.3**
	LoudMiner	**19**	**.2**	**.2**	**50.5**
	LOWBALL	**3**	**.0**	**.0**	**50.5**
	Lslsass	**1**	**.0**	**.0**	**50.5**
	Lucifer	**28**	**.3**	**.3**	**50.8**
	Lurid	**2**	**.0**	**.0**	**50.8**
	Machete	**45**	**.4**	**.4**	**51.2**
	MacMa	**27**	**.3**	**.3**	**51.5**
	macOS.OSAMiner	**12**	**.1**	**.1**	**51.6**
	MacSpy	**11**	**.1**	**.1**	**51.7**
	MailSniper	**3**	**.0**	**.0**	**51.8**
	Mandrake	**29**	**.3**	**.3**	**52.0**
	Marcher	**3**	**.0**	**.0**	**52.1**
	MarkiRAT	**26**	**.3**	**.3**	**52.3**
	Matryoshka	**15**	**.1**	**.1**	**52.5**
	MazarBOT	**2**	**.0**	**.0**	**52.5**
	Maze	**27**	**.3**	**.3**	**52.7**
	MCMD	**13**	**.1**	**.1**	**52.9**

	MechaFlounder	**8**	**.1**	**.1**	**52.9**
	meek	**1**	**.0**	**.0**	**53.0**
	MegaCortex	**19**	**.2**	**.2**	**53.1**
	Melcoz	**14**	**.1**	**.1**	**53.3**
	MESSAGETAP	**9**	**.1**	**.1**	**53.4**
	Metamorfo	**53**	**.5**	**.5**	**53.9**
	Meteor	**23**	**.2**	**.2**	**54.1**
	Micropsia	**18**	**.2**	**.2**	**54.3**
	Milan	**22**	**.2**	**.2**	**54.5**
	Mimikatz	**20**	**.2**	**.2**	**54.7**
	MimiPenguin	**1**	**.0**	**.0**	**54.7**
	Miner-C	**1**	**.0**	**.0**	**54.7**
	MiniDuke	**9**	**.1**	**.1**	**54.8**
	MirageFox	**7**	**.1**	**.1**	**54.9**
	Mis-Type	**20**	**.2**	**.2**	**55.1**
	Misdat	**17**	**.2**	**.2**	**55.2**
	Mivast	**5**	**.0**	**.0**	**55.3**
	MobileOrder	**7**	**.1**	**.1**	**55.3**
	MoleNet	**8**	**.1**	**.1**	**55.4**
	Mongall	**16**	**.2**	**.2**	**55.6**
	Monokle	**26**	**.3**	**.3**	**55.8**
	MoonWind	**17**	**.2**	**.2**	**56.0**
	More_eggs	**15**	**.1**	**.1**	**56.1**
	Mori	**9**	**.1**	**.1**	**56.2**
	Mosquito	**18**	**.2**	**.2**	**56.4**
	MURKYTOP	**11**	**.1**	**.1**	**56.5**
	Mythic	**13**	**.1**	**.1**	**56.6**
	Naid	**5**	**.0**	**.0**	**56.7**
	NanHaiShu	**13**	**.1**	**.1**	**56.8**
	NanoCore	**15**	**.1**	**.1**	**56.9**
	NativeZone	**7**	**.1**	**.1**	**57.0**
	NavRAT	**12**	**.1**	**.1**	**57.1**
	NBTscan	**6**	**.1**	**.1**	**57.2**
	nbtstat	**2**	**.0**	**.0**	**57.2**
	NDiskMonitor	**5**	**.0**	**.0**	**57.3**
	Nebulae	**19**	**.2**	**.2**	**57.4**
	Neoichor	**11**	**.1**	**.1**	**57.5**
	Nerex	**5**	**.0**	**.0**	**57.6**
	Net	**15**	**.1**	**.1**	**57.7**
	Net Crawler	**4**	**.0**	**.0**	**57.8**
	NETEAGLE	**12**	**.1**	**.1**	**57.9**

	netsh	**5**	**.0**	**.0**	**57.9**
	netstat	**1**	**.0**	**.0**	**58.0**
	NetTraveler	**3**	**.0**	**.0**	**58.0**
	Netwalker	**18**	**.2**	**.2**	**58.2**
	NETWIRE	**55**	**.5**	**.5**	**58.7**
	Ngrok	**5**	**.0**	**.0**	**58.7**
	Nidiran	**4**	**.0**	**.0**	**58.8**
	njRAT	**34**	**.3**	**.3**	**59.1**
	Nltest	**3**	**.0**	**.0**	**59.1**
	NOKKI	**17**	**.2**	**.2**	**59.3**
	NotCompatible	**1**	**.0**	**.0**	**59.3**
	NotPetya	**19**	**.2**	**.2**	**59.5**
	OBAD	**2**	**.0**	**.0**	**59.5**
	ObliqueRAT	**16**	**.2**	**.2**	**59.7**
	OceanSalt	**8**	**.1**	**.1**	**59.8**
	Octopus	**19**	**.2**	**.2**	**59.9**
	Okrum	**43**	**.4**	**.4**	**60.4**
	OLDBAIT	**6**	**.1**	**.1**	**60.4**
	OldBoot	**1**	**.0**	**.0**	**60.4**
	Olympic Destroyer	**14**	**.1**	**.1**	**60.6**
	OnionDuke	**5**	**.0**	**.0**	**60.6**
	OopsIE	**22**	**.2**	**.2**	**60.8**
	Orz	**14**	**.1**	**.1**	**61.0**
	OSInfo	**10**	**.1**	**.1**	**61.1**
	OSX_OCEANLOTUS.D	**23**	**.2**	**.2**	**61.3**
	OSX/Shlayer	**15**	**.1**	**.1**	**61.4**
	Out1	**5**	**.0**	**.0**	**61.5**
	OutSteel	**14**	**.1**	**.1**	**61.6**
	OwaAuth	**9**	**.1**	**.1**	**61.7**
	P.A.S. Webshell	**15**	**.1**	**.1**	**61.8**
	P2P ZeuS	**1**	**.0**	**.0**	**61.8**
	P8RAT	**7**	**.1**	**.1**	**61.9**
	Pallas	**16**	**.2**	**.2**	**62.1**
	Pandora	**18**	**.2**	**.2**	**62.2**
	Pasam	**8**	**.1**	**.1**	**62.3**
	Pass-The-Hash Toolkit	**2**	**.0**	**.0**	**62.3**
	Pay2Key	**8**	**.1**	**.1**	**62.4**
	PcShare	**23**	**.2**	**.2**	**62.6**
	Pegasus for Android	**12**	**.1**	**.1**	**62.8**
	Pegasus for iOS	**13**	**.1**	**.1**	**62.9**
	Peirates	**16**	**.2**	**.2**	**63.0**

	Penquin	**23**	**.2**	**.2**	**63.3**
	Peppy	**8**	**.1**	**.1**	**63.3**
	PHOREAL	**3**	**.0**	**.0**	**63.4**
	Pillowmint	**15**	**.1**	**.1**	**63.5**
	PinchDuke	**7**	**.1**	**.1**	**63.6**
	Ping	**1**	**.0**	**.0**	**63.6**
	PingPull	**16**	**.2**	**.2**	**63.7**
	PipeMon	**28**	**.3**	**.3**	**64.0**
	Pisloader	**10**	**.1**	**.1**	**64.1**
	PJApps	**4**	**.0**	**.0**	**64.2**
	PLAINTEE	**11**	**.1**	**.1**	**64.3**
	PLEAD	**15**	**.1**	**.1**	**64.4**
	PlugX	**35**	**.3**	**.3**	**64.7**
	pngdowner	**3**	**.0**	**.0**	**64.8**
	PoetRAT	**37**	**.4**	**.4**	**65.1**
	PoisonIvy	**19**	**.2**	**.2**	**65.3**
	PolyglotDuke	**9**	**.1**	**.1**	**65.4**
	Pony	**16**	**.2**	**.2**	**65.6**
	POORAIM	**6**	**.1**	**.1**	**65.6**
	PoshC2	**41**	**.4**	**.4**	**66.0**
	POSHSPY	**9**	**.1**	**.1**	**66.1**
	Power Loader	**2**	**.0**	**.0**	**66.1**
	PowerDuke	**16**	**.2**	**.2**	**66.3**
	PowerLess	**10**	**.1**	**.1**	**66.4**
	PowerPunch	**4**	**.0**	**.0**	**66.4**
	PowerShower	**15**	**.1**	**.1**	**66.6**
	POWERSOURCE	**7**	**.1**	**.1**	**66.6**
	PowerSploit	**44**	**.4**	**.4**	**67.1**
	PowerStallion	**5**	**.0**	**.0**	**67.1**
	POWERSTATS	**29**	**.3**	**.3**	**67.4**
	POWERTON	**8**	**.1**	**.1**	**67.5**
	PowGoop	**10**	**.1**	**.1**	**67.6**
	POWRUNER	**22**	**.2**	**.2**	**67.8**
	Prikormka	**24**	**.2**	**.2**	**68.0**
	ProLock	**8**	**.1**	**.1**	**68.1**
	Proton	**19**	**.2**	**.2**	**68.3**
	Proxysvc	**14**	**.1**	**.1**	**68.4**
	PS1	**6**	**.1**	**.1**	**68.5**
	PsExec	**6**	**.1**	**.1**	**68.5**
	Psylo	**5**	**.0**	**.0**	**68.6**
	Pteranodon	**21**	**.2**	**.2**	**68.8**

	PUNCHBUGGY	**19**	**.2**	**.2**	**69.0**
	PUNCHTRACK	**3**	**.0**	**.0**	**69.0**
	Pupy	**49**	**.5**	**.5**	**69.5**
	pwdump	**1**	**.0**	**.0**	**69.5**
	PyDCrypt	**11**	**.1**	**.1**	**69.6**
	Pysa	**16**	**.2**	**.2**	**69.7**
	QakBot	**73**	**.7**	**.7**	**70.4**
	QUADAGENT	**18**	**.2**	**.2**	**70.6**
	QuasarRAT	**29**	**.3**	**.3**	**70.9**
	QuietSieve	**9**	**.1**	**.1**	**71.0**
	Ragnar Locker	**14**	**.1**	**.1**	**71.1**
	Raindrop	**8**	**.1**	**.1**	**71.2**
	RainyDay	**30**	**.3**	**.3**	**71.5**
	Ramsay	**48**	**.5**	**.5**	**72.0**
	RARSTONE	**5**	**.0**	**.0**	**72.0**
	RATANKBA	**16**	**.2**	**.2**	**72.2**
	RawDisk	**3**	**.0**	**.0**	**72.2**
	RawPOS	**6**	**.1**	**.1**	**72.2**
	Rclone	**6**	**.1**	**.1**	**72.3**
	RCSAndroid	**11**	**.1**	**.1**	**72.4**
	RCSession	**27**	**.3**	**.3**	**72.7**
	RDAT	**21**	**.2**	**.2**	**72.9**
	RDFSNIFFER	**4**	**.0**	**.0**	**72.9**
	Reaver	**16**	**.2**	**.2**	**73.1**
	Red Alert 2.0	**13**	**.1**	**.1**	**73.2**
	RedDrop	**7**	**.1**	**.1**	**73.3**
	RedLeaves	**21**	**.2**	**.2**	**73.5**
	Reg	**3**	**.0**	**.0**	**73.5**
	RegDuke	**9**	**.1**	**.1**	**73.6**
	Regin	**13**	**.1**	**.1**	**73.7**
	Remcos	**21**	**.2**	**.2**	**73.9**
	Remexi	**21**	**.2**	**.2**	**74.1**
	RemoteCMD	**5**	**.0**	**.0**	**74.2**
	RemoteUtilities	**4**	**.0**	**.0**	**74.2**
	Remsec	**34**	**.3**	**.3**	**74.5**
	Responder	**4**	**.0**	**.0**	**74.6**
	Revenge RAT	**22**	**.2**	**.2**	**74.8**
	REvil	**35**	**.3**	**.3**	**75.1**
	RGDoor	**7**	**.1**	**.1**	**75.2**
	Rifdoor	**10**	**.1**	**.1**	**75.3**
	Riltok	**10**	**.1**	**.1**	**75.4**

	RIPTIDE	**2**	**.0**	**.0**	**75.4**
	Rising Sun	**19**	**.2**	**.2**	**75.6**
	ROADTools	**9**	**.1**	**.1**	**75.7**
	RobbinHood	**6**	**.1**	**.1**	**75.7**
	ROCKBOOT	**2**	**.0**	**.0**	**75.8**
	RogueRobin	**21**	**.2**	**.2**	**76.0**
	ROKRAT	**33**	**.3**	**.3**	**76.3**
	Rotexy	**17**	**.2**	**.2**	**76.5**
	route	**1**	**.0**	**.0**	**76.5**
	Rover	**12**	**.1**	**.1**	**76.6**
	RTM	**43**	**.4**	**.4**	**77.0**
	Ruler	**4**	**.0**	**.0**	**77.0**
	RuMMS	**4**	**.0**	**.0**	**77.1**
	RunningRAT	**11**	**.1**	**.1**	**77.2**
	Ryuk	**31**	**.3**	**.3**	**77.5**
	S-Type	**22**	**.2**	**.2**	**77.7**
	Saint Bot	**45**	**.4**	**.4**	**78.1**
	Sakula	**16**	**.2**	**.2**	**78.3**
	SamSam	**5**	**.0**	**.0**	**78.3**
	schtasks	**3**	**.0**	**.0**	**78.4**
	SDBbot	**28**	**.3**	**.3**	**78.6**
	SDelete	**2**	**.0**	**.0**	**78.7**
	SeaDuke	**22**	**.2**	**.2**	**78.9**
	Seasalt	**12**	**.1**	**.1**	**79.0**
	SEASHARPEE	**4**	**.0**	**.0**	**79.0**
	ServHelper	**16**	**.2**	**.2**	**79.2**
	Seth-Locker	**3**	**.0**	**.0**	**79.2**
	ShadowPad	**21**	**.2**	**.2**	**79.4**
	Shamoon	**32**	**.3**	**.3**	**79.7**
	Shark	**18**	**.2**	**.2**	**79.9**
	SharpStage	**14**	**.1**	**.1**	**80.0**
	SHARPSTATS	**7**	**.1**	**.1**	**80.1**
	ShiftyBug	**2**	**.0**	**.0**	**80.1**
	ShimRat	**26**	**.3**	**.3**	**80.4**
	ShimRatReporter	**16**	**.2**	**.2**	**80.5**
	SHIPSHAPE	**6**	**.1**	**.1**	**80.6**
	SHOTPUT	**6**	**.1**	**.1**	**80.6**
	SHUTTERSPEED	**3**	**.0**	**.0**	**80.7**
	Sibot	**19**	**.2**	**.2**	**80.9**
	SideTwist	**15**	**.1**	**.1**	**81.0**
	SILENTTRINITY	**59**	**.6**	**.6**	**81.6**

	SilkBean	**15**	**.1**	**.1**	**81.7**
	Siloscape	**15**	**.1**	**.1**	**81.9**
	SimBad	**3**	**.0**	**.0**	**81.9**
	Skeleton Key	**3**	**.0**	**.0**	**81.9**
	Skidmap	**21**	**.2**	**.2**	**82.1**
	Skygofree	**9**	**.1**	**.1**	**82.2**
	Sliver	**17**	**.2**	**.2**	**82.4**
	SLOTHFULMEDIA	**26**	**.3**	**.3**	**82.6**
	SLOWDRIFT	**3**	**.0**	**.0**	**82.7**
	Small Sieve	**14**	**.1**	**.1**	**82.8**
	Smoke Loader	**20**	**.2**	**.2**	**83.0**
	SMOKEDHAM	**23**	**.2**	**.2**	**83.2**
	SNUGRIDE	**5**	**.0**	**.0**	**83.3**
	Socksbot	**6**	**.1**	**.1**	**83.3**
	SodaMaster	**13**	**.1**	**.1**	**83.4**
	SombRAT	**25**	**.2**	**.2**	**83.7**
	SoreFang	**15**	**.1**	**.1**	**83.8**
	SOUNDBITE	**5**	**.0**	**.0**	**83.9**
	SPACESHIP	**8**	**.1**	**.1**	**84.0**
	Spark	**11**	**.1**	**.1**	**84.1**
	SpeakUp	**17**	**.2**	**.2**	**84.2**
	SpicyOmelette	**11**	**.1**	**.1**	**84.3**
	spwebmember	**1**	**.0**	**.0**	**84.3**
	SpyDealer	**15**	**.1**	**.1**	**84.5**
	SpyNote RAT	**7**	**.1**	**.1**	**84.6**
	sqlmap	**1**	**.0**	**.0**	**84.6**
	SQLRat	**10**	**.1**	**.1**	**84.7**
	Squirrelwaffle	**22**	**.2**	**.2**	**84.9**
	SslMM	**13**	**.1**	**.1**	**85.0**
	Starloader	**2**	**.0**	**.0**	**85.0**
	STARWHALE	**16**	**.2**	**.2**	**85.2**
	Stealth Mango	**15**	**.1**	**.1**	**85.3**
	StoneDrill	**17**	**.2**	**.2**	**85.5**
	StreamEx	**10**	**.1**	**.1**	**85.6**
	StrifeWater	**18**	**.2**	**.2**	**85.8**
	StrongPity	**28**	**.3**	**.3**	**86.0**
	Stuxnet	**55**	**.5**	**.5**	**86.6**
	SUGARDUMP	**15**	**.1**	**.1**	**86.7**
	SUGARUSH	**6**	**.1**	**.1**	**86.8**
	SUNBURST	**37**	**.4**	**.4**	**87.1**
	SUNSPOT	**12**	**.1**	**.1**	**87.3**

	SUPERNOVA	**5**	**.0**	**.0**	**87.3**
	Sykipot	**14**	**.1**	**.1**	**87.4**
	SynAck	**16**	**.2**	**.2**	**87.6**
	SYNful Knock	**6**	**.1**	**.1**	**87.6**
	Sys10	**6**	**.1**	**.1**	**87.7**
	SYSCON	**5**	**.0**	**.0**	**87.8**
	Systeminfo	**1**	**.0**	**.0**	**87.8**
	SysUpdate	**19**	**.2**	**.2**	**87.9**
	T9000	**16**	**.2**	**.2**	**88.1**
	Taidoor	**22**	**.2**	**.2**	**88.3**
	TAINTEDSCRIBE	**17**	**.2**	**.2**	**88.5**
	TajMahal	**26**	**.3**	**.3**	**88.7**
	Tangelo	**8**	**.1**	**.1**	**88.8**
	Tarrask	**10**	**.1**	**.1**	**88.9**
	Tasklist	**3**	**.0**	**.0**	**88.9**
	TDTESS	**6**	**.1**	**.1**	**89.0**
	TEARDROP	**7**	**.1**	**.1**	**89.1**
	TERRACOTTA	**19**	**.2**	**.2**	**89.2**
	TEXTMATE	**2**	**.0**	**.0**	**89.3**
	ThiefQuest	**22**	**.2**	**.2**	**89.5**
	ThreatNeedle	**14**	**.1**	**.1**	**89.6**
	Tiktok Pro	**23**	**.2**	**.2**	**89.8**
	TinyTurla	**13**	**.1**	**.1**	**90.0**
	TINYTYPHON	**5**	**.0**	**.0**	**90.0**
	TinyZBot	**12**	**.1**	**.1**	**90.1**
	Tomiris	**11**	**.1**	**.1**	**90.2**
	Tor	**2**	**.0**	**.0**	**90.3**
	Torisma	**13**	**.1**	**.1**	**90.4**
	TrailBlazer	**6**	**.1**	**.1**	**90.4**
	Triada	**9**	**.1**	**.1**	**90.5**
	TrickBot	**62**	**.6**	**.6**	**91.1**
	TrickMo	**16**	**.2**	**.2**	**91.3**
	Trojan-SMS.AndroidOS.Agent.ao	**1**	**.0**	**.0**	**91.3**
	Trojan-SMS.AndroidOS.FakeInst.a	**1**	**.0**	**.0**	**91.3**
	Trojan-SMS.AndroidOS.OpFake.a	**1**	**.0**	**.0**	**91.3**
	Trojan.Karagany	**26**	**.3**	**.3**	**91.6**

	Trojan.Mebromi	**2**	**.0**	**.0**	**91.6**
	Truvasys	**3**	**.0**	**.0**	**91.6**
	TSCookie	**14**	**.1**	**.1**	**91.8**
	Turian	**19**	**.2**	**.2**	**91.9**
	TURNEDUP	**8**	**.1**	**.1**	**92.0**
	Twitoor	**3**	**.0**	**.0**	**92.0**
	TYPEFRAME	**15**	**.1**	**.1**	**92.2**
	UACMe	**2**	**.0**	**.0**	**92.2**
	UBoatRAT	**10**	**.1**	**.1**	**92.3**
	Umbreon	**9**	**.1**	**.1**	**92.4**
	Unknown Logger	**10**	**.1**	**.1**	**92.5**
	UPPERCUT	**10**	**.1**	**.1**	**92.6**
	Uroburos	**2**	**.0**	**.0**	**92.6**
	Ursnif	**41**	**.4**	**.4**	**93.0**
	USBferry	**12**	**.1**	**.1**	**93.1**
	USBStealer	**16**	**.2**	**.2**	**93.3**
	Valak	**35**	**.3**	**.3**	**93.6**
	VaporRage	**4**	**.0**	**.0**	**93.7**
	Vasport	**5**	**.0**	**.0**	**93.7**
	VBShower	**6**	**.1**	**.1**	**93.8**
	VERMIN	**18**	**.2**	**.2**	**93.9**
	ViceLeaker	**14**	**.1**	**.1**	**94.1**
	ViperRAT	**12**	**.1**	**.1**	**94.2**
	Volgmer	**19**	**.2**	**.2**	**94.4**
	WannaCry	**17**	**.2**	**.2**	**94.5**
	WarzoneRAT	**34**	**.3**	**.3**	**94.9**
	WastedLocker	**25**	**.2**	**.2**	**95.1**
	Waterbear	**18**	**.2**	**.2**	**95.3**
	WEBC2	**5**	**.0**	**.0**	**95.3**
	WellMail	**9**	**.1**	**.1**	**95.4**
	WellMess	**15**	**.1**	**.1**	**95.6**
	Wevtutil	**3**	**.0**	**.0**	**95.6**
	WhisperGate	**32**	**.3**	**.3**	**95.9**
	Wiarp	**6**	**.1**	**.1**	**96.0**
	Windows Credential Editor	**1**	**.0**	**.0**	**96.0**
	WINDSHIELD	**5**	**.0**	**.0**	**96.0**
	WindTail	**14**	**.1**	**.1**	**96.2**
	WINERACK	**7**	**.1**	**.1**	**96.2**
	Winexe	**1**	**.0**	**.0**	**96.2**
	Wingbird	**14**	**.1**	**.1**	**96.4**

	WinMM	**6**	**.1**	**.1**	**96.4**
	Winnti for Linux	**9**	**.1**	**.1**	**96.5**
	Winnti for Windows	**24**	**.2**	**.2**	**96.7**
	Wiper	**2**	**.0**	**.0**	**96.8**
	WireLurker	**3**	**.0**	**.0**	**96.8**
	WolfRAT	**17**	**.2**	**.2**	**97.0**
	X-Agent for Android	**2**	**.0**	**.0**	**97.0**
	XAgentOSX	**11**	**.1**	**.1**	**97.1**
	Xbash	**19**	**.2**	**.2**	**97.3**
	Xbot	**5**	**.0**	**.0**	**97.3**
	xCaon	**12**	**.1**	**.1**	**97.4**
	xCmd	**1**	**.0**	**.0**	**97.4**
	XcodeGhost	**5**	**.0**	**.0**	**97.5**
	XCSSET	**34**	**.3**	**.3**	**97.8**
	XLoader for Android	**7**	**.1**	**.1**	**97.9**
	XLoader for iOS	**4**	**.0**	**.0**	**97.9**
	XTunnel	**8**	**.1**	**.1**	**98.0**
	YAHOYAH	**6**	**.1**	**.1**	**98.1**
	yty	**18**	**.2**	**.2**	**98.2**
	Zebrocy	**35**	**.3**	**.3**	**98.6**
	Zen	**10**	**.1**	**.1**	**98.7**
	ZergHelper	**1**	**.0**	**.0**	**98.7**
	Zeroaccess	**2**	**.0**	**.0**	**98.7**
	ZeroT	**17**	**.2**	**.2**	**98.9**
	Zeus Panda	**26**	**.3**	**.3**	**99.1**
	ZLib	**12**	**.1**	**.1**	**99.2**
	Zox	**9**	**.1**	**.1**	**99.3**
	zwShell	**14**	**.1**	**.1**	**99.5**
	ZxShell	**39**	**.4**	**.4**	**99.8**
	ZxxZ	**16**	**.2**	**.2**	**100.0**
	Total	**10306**	**100.0**	**100.0**	

APPENDIX D

MITRE CAPEC Attacks Patterns with Highest Assessed Risk

Category Name	Name	Description	Likelihood Of Attack	Typical Severity
Abuse Existing Functionality	**Overflow Binary Resource File**	**An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binary file. These attacks may pass unnoticed to the client machine through normal usage of files, such as a browser loading a seemingly innocent JPEG file. This can allow the adversary access to the execution stack and execute arbitrary code in the target process.**	**High**	**Very High**
Abuse Existing Functionality	**String Format Overflow in syslog()**	**This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be placed in the format string parameter leading to a format string injection attack. Adversaries can then inject malicious format string commands into the function call leading to a buffer overflow. There are many reported software vulnerabilities with the root cause being a misuse of the syslog() function.**	**High**	**Very High**
Abuse Existing Functionality	**Manipulating Web Input to File System Calls**	**An attacker manipulates inputs to the target software which the target software passes to file system calls in the OS. The goal is to gain access to, and perhaps modify, areas of the file system that the target software did not intend to be accessible.**	**High**	**Very High**

Abuse Existing Functionality	**Overflow Buffers**	**Buffer Overflow attacks target improper or missing bounds checking on buffer operations, typically triggered by input injected by an adversary. As a consequence, an adversary is able to write past the boundaries of allocated buffer regions in memory, causing a program crash or potentially redirection of execution as per the adversaries' choice.**	**High**	**Very High**
Abuse Existing Functionality	**Path Traversal**	**An adversary uses path manipulation methods to exploit insufficient input validation of a target to obtain access to data that should be not be retrievable by ordinary well-formed requests. A typical variety of this attack involves specifying a path to a desired file together with dot-dot-slash characters, resulting in the file access API or function traversing out of the intended directory structure and into the root file system. By replacing or modifying the expected path information the access function or API retrieves the file desired by the attacker. These attacks either involve the attacker providing a complete path to a targeted file or using control characters (e.g. path separators (/ or) and/or dots (.)) to reach desired directories or files.**	**High**	**Very High**
Collect and Analyze Information	**Retrieve Embedded Sensitive Data**	**An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials that can be used as an intermediate step in a larger attack.**	**High**	**Very High**

Engage in Deceptive Interactions	**Leveraging/Manipulating Configuration File Search Paths**	**This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The adversary can either modify the search path a program uses, like a PATH variable or classpath, or they can manipulate resources on the path to point to their malicious components. J2EE applications and other component based applications that are built from multiple binaries can have very long list of dependencies to execute. If one of these libraries and/or references is controllable by the attacker then application controls can be circumvented by the attacker.**	**High**	**Very High**
Engage in Deceptive Interactions	**Pharming**	**A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these supposedly trusted sites and have the victim be directed to their site rather than the originally intended one. Pharming does not require script injection or clicking on malicious links for the attack to succeed.**	**High**	**Very High**
Engage in Deceptive Interactions	**Phishing**	**Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or fishing for information.**	**High**	**Very High**

Engage in Deceptive Interactions	**Redirect Access to Libraries**	**An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of attack allows the adversary to compromise the application or server via the execution of unauthorized code. An application typically makes calls to functions that are a part of libraries external to the application. These libraries may be part of the operating system or they may be third party libraries. If an adversary can redirect an application's attempts to access these libraries to other libraries that the adversary supplies, the adversary will be able to force the targeted application to execute arbitrary code. This is especially dangerous if the targeted application has enhanced privileges. Access can be redirected through a number of techniques, including the use of symbolic links, search path modification, and relative path manipulation.**	**High**	**Very High**
Engage in Deceptive Interactions	**Action Spoofing**	**An adversary is able to disguise one action for another and therefore trick a user into initiating one type of action when they intend to initiate a different action. For example, a user might be led to believe that clicking a button will submit a query, but in fact it downloads software. Adversaries may perform this attack through social means, such as by simply convincing a victim to perform the action or relying on a user's natural inclination to do so, or through technical means, such as a clickjacking attack where a user sees one interface but is actually interacting with a second, invisible, interface.**	**High**	**Very High**

Engage in Deceptive Interactions	**DNS Rebinding**	**An adversary serves content whose IP address is resolved by a DNS server that the adversary controls. After initial contact by a web browser (or similar client), the adversary changes the IP address to which its name resolves, to an address within the target organization that is not publicly accessible. This allows the web browser to examine this internal address on behalf of the adversary.**	**High**	**Very High**
Inject Unexpected Items	**XSS Targeting Non-Script Elements**	**This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CDATA->), etc. These tags may not be subject to the same input validation, output validation, and other content filtering and checking routines, so this can create an opportunity for an adversary to tunnel through the application's elements and launch a XSS attack through other elements. As with all remote attacks, it is important to differentiate the ability to launch an attack (such as probing an internal network for unpatched servers) and the ability of the remote adversary to collect and interpret the output of said attack.**	**High**	**Very High**

Inject Unexpected Items	**File Content Injection**	**An adversary poisons files with a malicious payload (targeting the file systems accessible by the target software), which may be passed through by standard channels such as via email, and standard web content like PDF and multimedia files. The adversary exploits known vulnerabilities or handling routines in the target processes, in order to exploit the host's trust in executing remote content, including binary files.**	**High**	**Very High**
Inject Unexpected Items	**Manipulating Writeable Terminal Devices**	**This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter and thereby execute the malicious command with their privileges. The attacker can send the results (such as copying /etc/passwd) to a known directory and collect once the attack has succeeded.**	**High**	**Very High**
Inject Unexpected Items	**Cross-Site Scripting (XSS)**	**An adversary embeds malicious scripts in content that will be served to web browsers. The goal of the attack is for the target software, the client-side browser, to execute the script with the users' privilege level. An attack of this type exploits a programs' vulnerabilities that are brought on by allowing remote hosts to execute code and scripts. Web browsers, for example, have some simple security controls in place, but if a remote attacker is allowed to execute scripts (through injecting them into user-generated content like bulletin boards) then these controls may be bypassed. Further, these attacks are very difficult for an end user to detect.**	**High**	**Very High**

Inject Unexpected Items	**XQuery Injection**	**This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data that is passed to XQuery commands to traverse and execute commands that the XQuery routines have access to. XQuery injection can be used to enumerate elements on the victim's environment, inject commands to the local host, or execute queries to remote files and data sources.**	**High**	**Very High**
Inject Unexpected Items	**XSS Through HTTP Headers**	**An adversary exploits web applications that generate web content, such as links in a HTML page, based on unvalidated or improperly validated data submitted by other actors. XSS in HTTP Headers attacks target the HTTP headers which are hidden from most users and may not be validated by web applications.**	**High**	**Very High**
Inject Unexpected Items	**SQL Injection through SOAP Parameter Tampering**	**An attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack. On the service provider side, the SOAP message is parsed and parameters are not properly validated before being used to access a database in a way that does not use parameter binding, thus enabling the attacker to control the structure of the executed SQL query. This pattern describes a SQL injection attack with the delivery mechanism being a SOAP message.**	**High**	**Very High**

Inject Unexpected Items	**DOM-Based XSS**	**This type of attack is a form of Cross-Site Scripting (XSS) where a malicious script is inserted into the client-side HTML being parsed by a web browser. Content served by a vulnerable web application includes script code used to manipulate the Document Object Model (DOM). This script code either does not properly validate input, or does not perform proper output encoding, thus creating an opportunity for an adversary to inject a malicious script launch a XSS attack. A key distinction between other XSS attacks and DOM-based attacks is that in other XSS attacks, the malicious script runs when the vulnerable web page is initially loaded, while a DOM-based attack executes sometime after the page loads. Another distinction of DOM-based attacks is that in some cases, the malicious script is never sent to the vulnerable web server at all. An attack like this is guaranteed to bypass any server-side filtering attempts to protect users.**	**High**	**Very High**
Inject Unexpected Items	**Reflected XSS**	**This type of attack is a form of Cross-Site Scripting (XSS) where a malicious script is reflected off a vulnerable web application and then executed by a victim's browser. The process starts with an adversary delivering a malicious script to a victim and convincing the victim to send the script to the vulnerable web application.**	**High**	**Very High**

Inject Unexpected Items	**Stored XSS**	**An adversary utilizes a form of Cross-site Scripting (XSS) where a malicious script is persistently stored within the data storage of a vulnerable web application as valid input.**	**High**	**Very High**
Manipulate Data Structures	**Buffer Manipulation**	**An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space itself that is the target of the attack rather than any code responsible for interpreting the content of the buffer. In virtually all buffer attacks the content that is placed in the buffer is immaterial. Instead, most buffer attacks involve retrieving or providing more input than can be stored in the allocated buffer, resulting in the reading or overwriting of other unintended program memory.**	**High**	**Very High**
Manipulate System Resources	**Leverage Executable Code in Non-Executable Files**	**An attack of this type exploits a system's trust in configuration and resource files. When the executable loads the resource (such as an image file or configuration file) the attacker has modified the file to either execute malicious code directly or manipulate the target process (e.g. application server) to execute based on the malicious configuration parameters. Since systems are increasingly interrelated mashing up resources from local and remote sources the possibility of this attack occurring is high.**	**High**	**Very High**

Manipulate System Resources	**Poison Web Service Registry**	**SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester to a malicious service provider, provide incorrect information in schema or metadata, and delete information about service provider interfaces.**	**High**	**Very High**
Manipulate System Resources	**Manipulating Writeable Configuration Files**	**Generally these are manually edited files that are not in the preview of the system administrators, any ability on the attackers' behalf to modify these files, for example in a CVS repository, gives unauthorized access directly to the application, the same as authorized users.**	**High**	**Very High**
Subvert Access Control	**Subverting Environment Variable Values**	**The adversary directly or indirectly modifies environment variables used by or controlling the target software. The adversary's goal is to cause the target software to deviate from its expected operation in a manner that benefits the adversary.**	**High**	**Very High**
Subvert Access Control	**Using Malicious Files**	**An attack of this type exploits a system's configuration that allows an adversary to either directly access an executable file, for example through shell access; or in a possible worst case allows an adversary to upload a file and then execute it. Web servers, ftp servers, and message oriented middleware systems which have many integration points are particularly vulnerable, because both the programmers and the administrators must be in synch regarding the interfaces and the correct privileges for each interface.**	**High**	**Very High**

Subvert Access Control	**Cross Site Request Forgery**	**An attacker crafts malicious web links and distributes them (via web pages, email, etc.), typically in a targeted manner, hoping to induce users to click on the link and execute the malicious action against some third-party application. If successful, the action embedded in the malicious link will be processed and accepted by the targeted application with the users' privilege level. This type of attack leverages the persistence and implicit trust placed in user session cookies by many web applications today. In such an architecture, once the user authenticates to an application and a session cookie is created on the user's system, all following transactions for that session are authenticated using that cookie including potential actions initiated by an attacker and simply riding the existing session cookie.**	**High**	**Very High**
Subvert Access Control	**Target Programs with Elevated Privileges**	**This attack targets programs running with elevated privileges. The adversary tries to leverage a vulnerability in the running program and get arbitrary code to execute with elevated privileges.**	**High**	**Very High**
Subvert Access Control	**Manipulating User-Controlled Variables**	**This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the application server without any data sanitization. In extreme cases, the adversary can change variables controlling the business logic of**	**High**	**Very High**

		the application. For instance, in languages like PHP, a number of poorly set default configurations may allow the user to override variables.		
Subvert Access Control	**Adversary in the Middle (AiTM)**	**An adversary targets the communication between two components (typically client and server), in order to alter or obtain data from transactions. A general approach entails the adversary placing themself within the communication channel between the two components.**	**High**	**Very High**
Subvert Access Control	**Session Hijacking**	**This type of attack involves an adversary that exploits weaknesses in an application's use of sessions in performing authentication. The adversary is able to steal or manipulate an active session and use it to gain unathorized access to the application.**	**High**	**Very High**
Subvert Access Control	**Adversary in the Browser (AiTB)**	**An adversary exploits security vulnerabilities or inherent functionalities of a web browser, in order to manipulate traffic between two endpoints.**	**High**	**Very High**