Computer and Cyber Security: Principles, Algorithm, Applications and Perspectives

A Bio-inspired Approach to Cyber Security

Siyakha N Mthunzi

Elhadj Benkhelifa

Tomasz Bosakowski

Salim Hariri

Abstract

Owing to a growing reliance on information, technology and connectivity, Cyberspace has become the lifeline and interactive place for modern life. As such, Cyber security challenges are a global phenomenon whose adverse implications are catastrophic. Cyberspace is complex and unpredictable; its global connectedness and an explosion of data increases the threat surface as cyber infrastructures become highly complex and dynamic. Managing, i.e. ensuring and assuring security in cyberspace requires inspiration from advanced complex systems. Through evolution, nature has developed natural propensities in complex systems (*including animalia and plants)* that enable survival through adaptation. Predation-avoidance and anti-predation techniques employed by non-extinct preys could be exploited/adopted as mechanisms for adaptation through their application in Cyber security. This chapter presents an overall review of the current state of the Cyber security landscape. In addition, it demonstrates through further review, significant trends towards bio-inspired approaches as unconventional solutions to problems in other fields. Drawing from survivable preys in nature, the chapter speculates solutions for Cyberspace and Cyber security as follows; given an old problem (P_{old}) with an old solutions (S_{old}), a new problem (P_{new})

can be conceptualized with new partial and perhaps null solutions (S_{new}) in the solutions space S_{old} to S_{new}.

Keywords**: **Bio-inspired, Artificial Life, Cyber security, Cyberdefense, Autonomic Computing, Survivability, Cloud Computing, Machine Learning, Predator-Prey.

Introduction

With little consensus on definitions to concepts such as cyber security, cyberspace and most "things" cyber [1], addressing cyber security is often inadequate due to its misinterpretations and mistranslations. Across literature, there is convergence in the view that cyber security unlike traditional computer security, lacks the defining clarity of what the "cyber" prefix contributes to the general security concept [1] and is perhaps a source of confusion and misunderstanding across various perspectives [2]. In recognition of this lack of consensus, the authors of this chapter find it prudent for a general outline to the current cyber security definition landscape to be surmised; from academia, industry, government and across professionals in general. A conception of cyber security encompassing network and communication infrastructures and the human actor/user suggests cyber security in the context of the security of anything (including physical artefacts) that interacts with computer networks and communication infrastructures. The UK government for instance, defines cyber security as "an interactive domain for digital networks across the world" [3]. Clearly, this view pivots the general citizenry at the crux of the security objective. The significance of the human actor/factor is evidenced in the European Commission's prediction of a major global breakdown in electronic communication services and networks (costing around €193 billion) due to malicious human action and terrorist attacks. An "inclusive" definition of cyber security is posited by [2] as "the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data assets used in

cyberspace. This context of the cyber security concept includes guidelines, policies and collection of safeguards, technologies, tools and training to provide best protection for cyber environments and their users.

This chapter considers Cyber Security as a continuum of technologies and innovations for ensuring and assuring the security of data and networking technologies. It identifies the complexity and dynamic context of cyberspace as central to mitigating catastrophic cyber threats and attacks, by drawing inspiration from nature's complex and dynamic systems. This chapter explores how natural phenomenon in complex systems (*including animalia and plants)* that have survived through evolution, could be exploited as mechanisms for adaptive mitigation in complex cyber environments. Drawing from predation avoidance and anti-predation techniques employed by non-extinct prey animals and plants, this chapter hypothesizes how prey-inspired survivability could be adopted in cyber systems design and implementation.

1. Introduction

Recent years have witnessed an exponential increase in cybercrime, arguably exacerbated by the adoption of emerging technologies such as IoT and cloud computing and. In 2015 alone, most of breaches considered as hacking incidents targeted customers' bank details, addresses and other personal information. Over the years, hacking incidents have grown to encompass all aspects of a modern economy including transport, energy, banking, healthcare, telecommunications and in some instances, government organizations. Cyber hacking incidents including German and UK telecommunications giants Vodafone [4] and TalkTalk [5], respectively, act as perfect examples of

the scale, frequency and implication of such attacks. Most recently in the UK, Dixons Carphone suffered a huge data breach involving 5.9 million payment cards and 1.2 million personal data records [6]. These breaches raise concerns about the readiness of security solutions in an environment of highly sophisticated, persistent and motivated adversaries, particularly if considered against their implications on utilities such as power, transport, etc. With new inventions in smart health, and healthcare being a sensitive area, security in such sectors is critical [7].

Traditional computer network environments allow for highly manageable security processes, able to constrain user permissions, restrict software, roll out updates across campuses, centrally manage intrusion detection and control network traffic through firewall policies. Routing and other reactive approaches ensure efficient and effective control of the security of networks and devices. Thus, the degree of control in meeting security goals varies considerably between use-case and environment. Regardless, this fine-tuned control allows at the minimum, adequate logging and understanding of large, networked environments. However, with the advent and wide use of cyberspace, security is arguably more complex and requires different processes to maintain data confidentiality, integrity, availability (CIA) and systems stability. Technologies such as IoT and Big Data among others, make traditional firewall deployment a challenge, not least because of bandwidth and power wastage on devices in a multi-hoping routing environment under a Denial of Service attacks (DoS), but enforcing static security policies in highly mobile environment adds additional challenges. This nearly impossible in cyber environments with a range of mobile and non-mobile devices and various communication interfaces, and networks are formed in a variety of manners, forms and structures. Furthermore, it can be argued that the CIA triage, an industry standard addressing the security domain [8], is deficient in the cyber domain. As [9] notes, other

information characteristics attributed to cyber environments ought to be added to the CIA model [9].

Cyberspace's vision of complex and highly dynamic network and communication environments can be summarized as isolated nodes which are at risk from a variety of security threats including forced networking for malicious purposes. Thus, the potential for cyber security requires a novel type of security system to help defend it. As the security crisis in cyberspace escalates and the frequency and complexity of the latest vulnerabilities and cyber-attacks increases, the mandate to adopt more effective solutions will grow in importance to implement simplified, animated and cost-effective cyber solutions. This should contribute to the productivity of existing solutions including the human information security professional. Moreover, existing traditional security technologies such as firewalls, anti-virus scanners and user access control aid in restricting known threats. However, without additional intelligent components to oversee and integrate with the effectiveness of these security controls (as is the case in enterprise networks), if any of these are subverted, the results as has been shown are catastrophic.

2. Cyberspace

To examine the cyber landscape, it is important to understand the complexity that characterizes cyberspace. Complexity is a phenomenon that can be observed in a variety of systems, including physical and living systems. While a complete and unanimous definition of complexity is somewhat contentious across domains [10], the discussions in this chapter revolve around the scientific definition posited by [10]. Complex systems describe "phenomena, structure, aggregates, organisms, or problems that share the following common themes: they are inherently complicated or intricate, they are rarely completely deterministic, mathematical models of the system are usually

complex and involve non-linear, ill-posed, or chaotic behavior, and the systems are predisposed to unexpected outcomes (emergent behavior)" [10].

- While large-scale networks are inherently complex and true for cyberspace and cyber security [11], complexity itself is a useful concept in designing robust systems [12]. In this chapter, complexity in cyberspace describes the general sense of a system whose components are by design or function or both, challenging to verify. In fact, the current chapter postulates complexity in cyberspace in relation to interactions within networks and communication systems, including system users and misusers and the unpredictability of emerging behaviors. As noted by [12], complex systems are such that interactions among systems components could be unintended, for instance, unintended interaction with system data which result in unpredictable system outputs and emergent behaviours not intended for that system. And as literature will demonstrate in the sections below, unpredictability is perhaps an inevitable attribute of cyberspace and its related technologies. Figure 1 illustrates the scale of cyberspace; technologies, network and communication systems and other paradigms. This figure is not intended to represent an exhaustive view of the entire cyber domain but to provide illustrative examples. These will be briefly described in bullet points below.
- Cloud computing is the de-facto computing platform and enabler of emerging technologies; emerging technologies such as Bitcoin
- The Internet of Things (IoT) [13][14], [15] [16] heralds a vision of internet connected things; physical, and via a network be able to exchange local and global information (themselves and their environments, respectively). IoT technology thus enables further innovations and services based upon to immediate access to the said generated information.

- Critical infrastructure: Health, water and transport among many
- Contested environments and Cyber warfare have become critical in this new era

Computer and communication networks

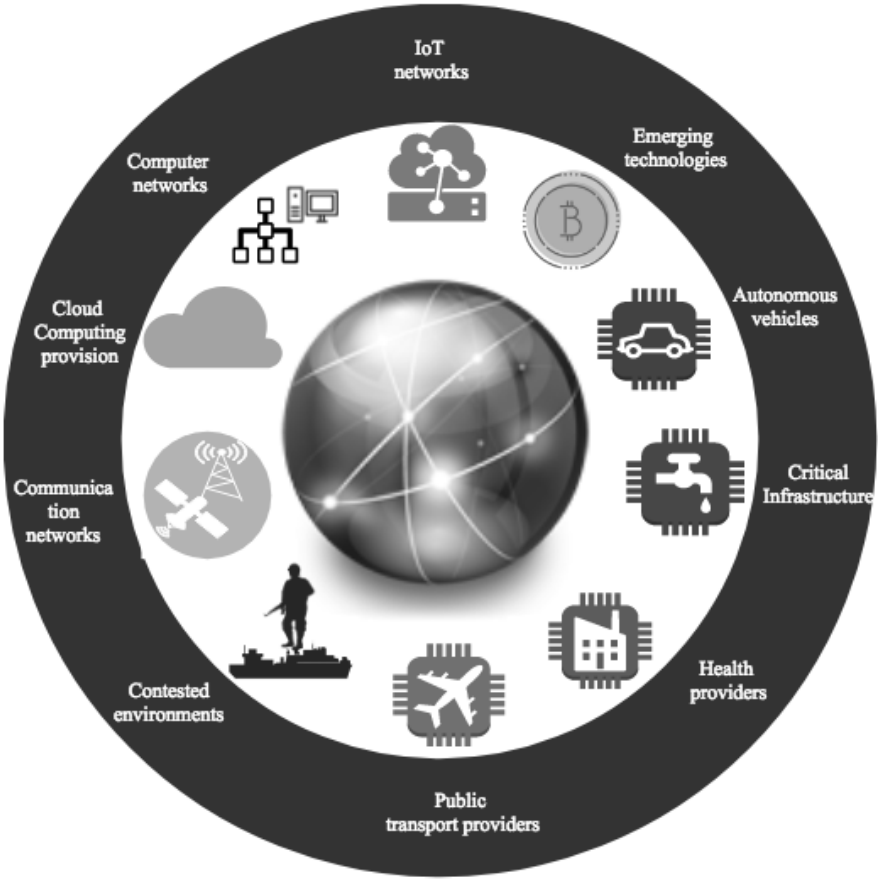

Figure 1. Illustration of cyberspace

Complex systems develop on a microscale through evolution. In evolution, selection pertains to those attributes that fosters organisms' survival benefits or disadvantages [17]. For instance, herbivorous mammals whose habitat has tall trees with the most nutrition and fruits atop, are likely to survive and reproduce if they are tall with long necks or can climb up trees. Similarly, elements within complex systems are generally subject to selection, whereupon those best suited for the environment are chosen. For example, products in a free market economy are selected through market forces, politicians in a democracy through elections/voting and animals through

natural pressures such as predation and competition. Complex natural systems are plentiful with complex patterns of behaviour (e.g. adaptation and learning) emanating from interactions among autonomous entities [18]. An example is the adaptation of memory and the self-learning mechanism employed by B-cells in identifying and destroying pathogens in the natural immune system [19]. Thus, adaptation facilitates change in response to changes within an environment. Using feedback loops, small changes in input information often can trigger large-scale outputs.

Figure 2 illustrates the transformation of a set of components to a network of connected and interdependent components. The graphic on the left shows the building components of a system; a set of autonomous components. Its transformation; graphic on the right, represents a complex system in which autonomous components (numerous) which grow exponentially are connected (dotted lines) and interdependent (black note at edge of dotted line). The nature of their connectivity defines the complexity of the system (in the global sense) rather than its characteristics. Autonomy enables components to adapt through local instructions and collectively synchronize (through cooperation and coordination) individual statuses resulting in a bottom-up form of order.

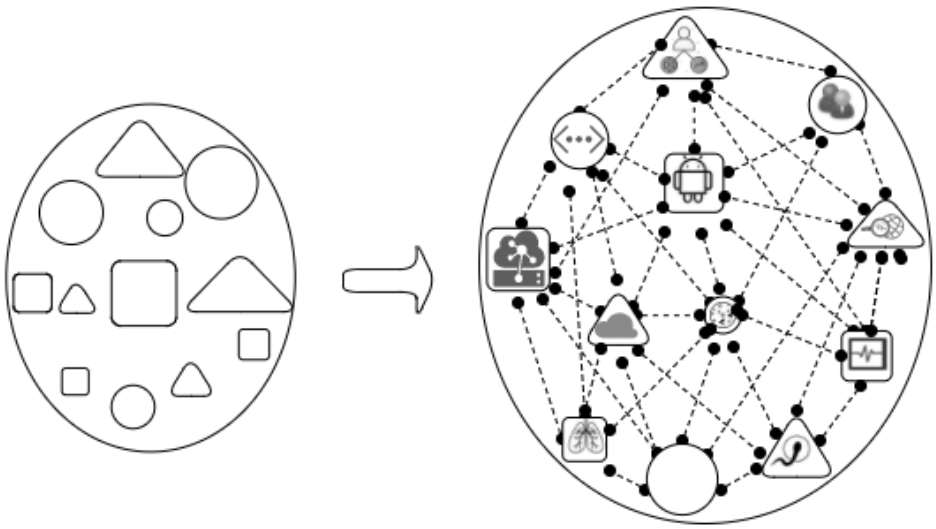

Figure 2. Illustrating the formation of complex systems: Non-linear, connected, interdependent and adaptive

With current innovation trends in cyberspace and the proliferation of new devices and platforms with multiparty collaborations, particularly involving third parties, coordinating and controlling interactions among these parties is often error prone. The unpredictable and dynamic nature of complex environments such as cloud computing (itself a subset of cyberspace) requires intelligent systems control. Whereas traditional computing systems generally maintained consistent control over inherent processes, control theory's [20] classical methodologies and assumptions provides better insight into handling control. The basic premise of control theory is motivated by enhanced adaptation in the presence of extreme unpredictable and dynamic changes [21]. Nonetheless, in non-linear and dynamic cyber environments, the control paradigm ought to be adaptable and dynamically configurable and/or re-configurable. Among a huge state-of-the art, a classification by the authors in [22] identifies characteristics for such self-adaption and these are outlined below as:

- Goals: objectives a system should achieve, e.g. evolution, flexibility, multiplicity, duration, etc.
- Change: the cause of adaptation, e.g. source, type, frequency, anticipation, etc.
- Mechanism: the system's response towards e.g. autonomy, scope, duration, timeliness, etc.
- Effect: the impact of adaptions upon the system, e.g. critical, predictability, resilience, etc.

If it is acceptable therefore that cyberspace is complex and therefore falls within the realm of complex systems described above, cyber security research should perhaps seek inspiration from well-established complex adaptive systems such as those in nature. Along this thrust, it is important to distinguish the cyber domain according to the its component sub-domains and investigate cyber security challenges.

2.1 Cyber security challenges

Cyber security unlike traditional information security in not only a process, but also a product and/or technology. As [9] demonstrates, the cyber domain encompasses characteristics beyond those commonly described by a traditional CIA triage, e.g. warfare, bullying, terrorism, etc. A home automation system for instance, can be compromised without affecting the victim's information (this falls outside the CIA triage and common security attributes), but through targeting the victim's other assets (i.e. cybercrime). Thus, cyber security pertains to the protection of asserts beyond those commonly referred to as information, including humans, the interests of nations states and societies, to household appliances, etc. One may logically conclude perhaps, that cyber security extends to ethical issues related to its asserts just as much as the legal. A range of other such dimensions are presented in NATO's National cyber security framework manual [3] and demonstrate the complexity of cyber security.

On the other hand, traditional computing infrastructures meant that security controls were managed within a contained systems [23] and static environments. In this sense, protections against threats was designed and planned for based on the assumption that outcomes of security solutions were linearly related to threat. For instance, [24]'s game theoretic approach to protect critical infrastructure against terrorist threats assumes an initial threat score for a particular target according

to original and inherent countermeasures relevant to that threat. Based on this assumption, they suggest that choices of subsequent solutions will decrease the overall threat. Whilst in a general systems theoretic sense, functions that convert inputs into required system outputs can be designed and controlled given that all inputs are provided [25], literature shows that the complexity of cyberspace limits the amount of initial threat knowledge cyber security solutions have. It has been demonstrated that sophisticated and persistent adversaries and zero-day attacks are able to systematically plan their attacks and persist within the compromised networks [26]. Cyberspace enables adversaries to increase their attack surface thus complicating vulnerability management and elevates the attack complexity. Cases in point include Stuxnet, Flame and Duqu, which obfuscated network traffic to evade detection [27]. Based upon the foregoing, this section identifies complexity as central to future cyber security solutions research.

Thus, the thrust of future cyber security should aim to reduce complexity to the human cyber security solution (professionals) and build integrated solution capable of mitigating rapid evolving cyber threats. Current approaches (generally top-down) to cyber security, where extensive efforts focus upon cyber security policy and regulations are inherently inadequate [28] as high-level failure or inadequacy is passed down to low-level elements in cyberspace (including the user and society). On the other hand, further extensive work in academia and industry has been devoted to designing attack and defense tools to efficiently counter cyber security threats. For instance, countermeasures integrated into network protocols to ensure reliable information exchange [29]. While these approaches are sufficient for mitigating cyber security threats, it also means that the governance of cyber security risk is harder to implement. Moreover, as literature suggests that countermeasures remain inadequate [30],

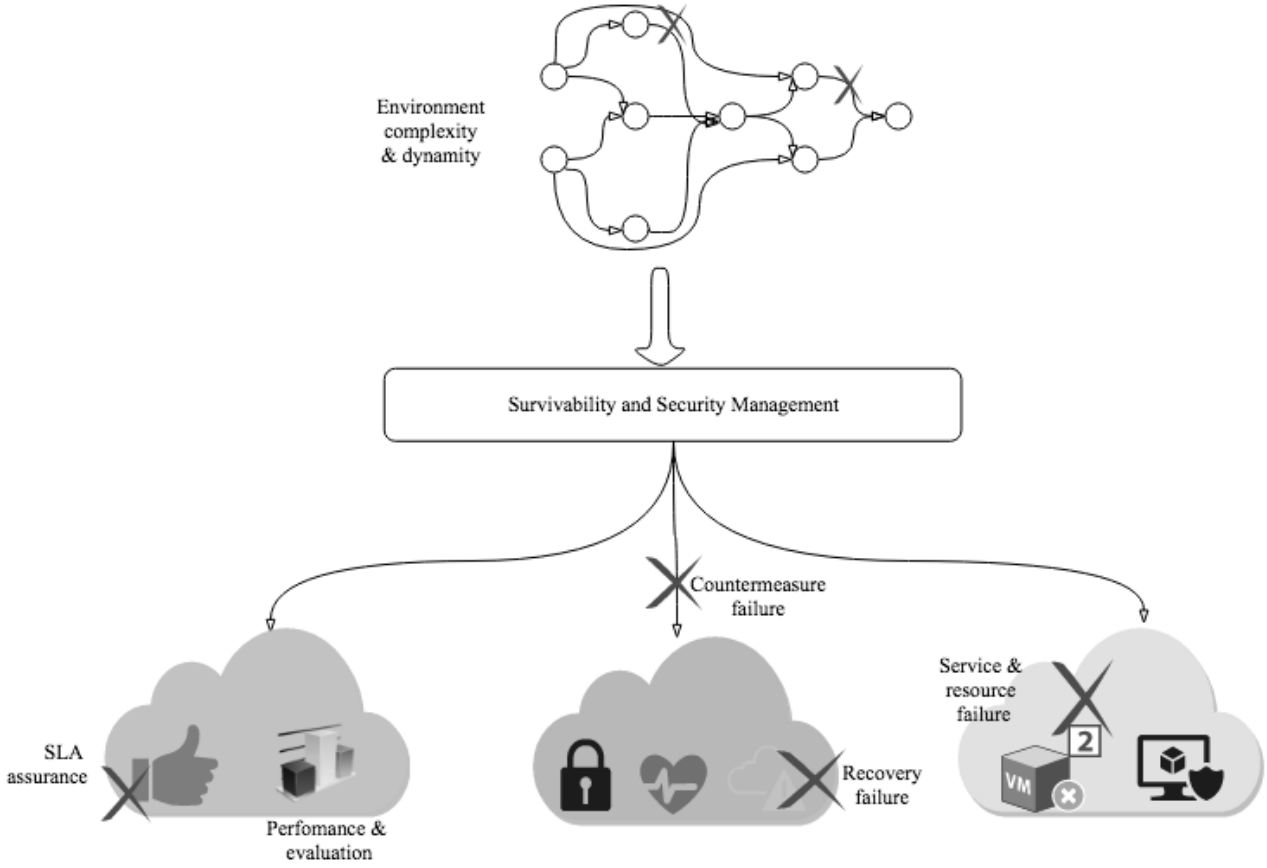

Figure 1-3. Research challenges for cyber security

Figure 3 illustrates the foregoing and highlight existing research challenges for cyber security. In this graphic, cyberspace complexity and dynamity introduce data control failure issues and adaption failure issues to cyber security (top of graphic). Furthermore, service and resource failure remain a major area of concern [31] [32]. In addition, assurance, performance and evaluation remain a constant challenge [33].

Now classified as a "tier one" threat to national security by British government [34] [35], this shift in strategy at a national level suggests the significance of cyber security. Cyberattacks such as those in Iraq [36], Iran [37] and during the "Arab Spring" [38] undoubtedly demonstrate possible implications in future cyberattacks. On the international stage, the United Nations Group

of Governmental Experts [39] and [40] formally recognised the applicability of international law in relation to cyber activities and cyber issues in the context of international security. Nonetheless, despite a clear consensus as to the applicability of international law, adequately established state practices presents a significant challenge to application of cyber security laws [41].

Existing security frameworks including Cloud Security Alliance (CSA)[1], National Institute of Standards and Technology (NIST)[2], the European Network and Information Security Agency (ENISA)[3], the UK's Centre of the Protection of National Infrastructure (CPNI)[4], etc. focus upon methods for cyber security which aim to among other things, consolidate security risks and vulnerabilities. These frameworks aim to provide best practice guidelines for mitigating cyber threats. Table 1 below shows example core standardization areas in key cyberspace applications. This is not intended as an exhaustive table, neither for the standardization areas or key cyber application areas. However, of interest to the authors of this Chapter, is a clear demonstration to the urgent need for adequate cyber security (cyber incident management) standardization.

Table 1-1. Example core standardization areas in key cyberspace applications

Core Areas of Cyber security Standardization	Examples of Relevant SDOs	Examples of Some Key Applications				
		Cloud Computing	Emergency Management	Industrial Control	Health IT	Smart Grid
Cryptographic Techniques	IEEE; ISO TC 68 ISO/IEC JTC 1 W3C	Standards Mostly	Some Standards	Some Standards	Some Standards	Some Standards

[1] *https://cloudsecurityalliance.org/group/security-guidance/*
[2] *https://cloudsecurityalliance.org/group/security-guidance/*
[3] *https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf*
[4] *https://www.cpni.gov.uk/*

		Available	Available	Available	Available	Available
Cyber Incident Management	ISO/IEC JTC 1 ITU-T PCI	Some Standards Available	New Standards Needed	Some Standards Available	Some Standards Available	Some Standards Available
Identity and Access Management	FIDO Alliance; IETF; OASIS OIDF ISO/IEC JTC 1 ITU-T; W3C	Standards Mostly Available	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed
Information Security Management Systems	ATIS; IEC; ISA ISO/IEC JTC 1 ISO TC 223 OASIS; The Open Group	Some Standards Available	New Standards Needed	Some Standards Available	Some Standards Available	New Standards Needed
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group	Some Standards Available	Standards Mostly Available	Some Standards Available	Some Standards Available	Some Standards Available
Network Security	3GPP; IETF; IEEE; ISO/IEC JTC 1 ITU -T; The Open	Some Standards	Some Standards	Some Standards	Some Standards	Some Standards

	Group; WiMAX Forum	Available	Available	Available	Available	Available
Security Automation & Continuous	IEEE; IETF ISO/IEC JTC 1 TCG; The Open Group	Some Standards Available	Some Standards Available	New Standards Needed	Some Standards Available	New Standards Needed
Monitoring Software Assurance	IEEE; ISO/IEC JTC 1 OMG TCG; The Open Group	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available
Supply Chain Risk Management	IEEE ISO/IEC JTC 1 IEC TC 65 The Open Group	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available	Some Standards Available
System Security Engineering	IEC; IEEE; ISA ISO/IEC JTC 1 SAE International The Open Group	Some Standards Available	Standards Mostly Available	Some Standards Available	Some Standards Available	Some Standards Available

The US DoD [42] defines cyberspace intelligence, surveillance and reconnaissance as activities in cyberspace which result in the gathering of intelligence to support current and future

operations. [43] subsequently draws parallels between this definition and that of espionage, which is defined as being "the unauthorized intentional collection of information by states". Whilst the impact of espionage in cyberspace is typically perceived to be less severe than that of offensive cyber operations, the hacking of the US Democratic National Committee's emails in 2016 demonstrates that such activities are still capable of causing significant damage [44]. Furthermore, evidence provided by [45] highlights the pervasiveness of economic and commercial espionage in cyberspace, with likely state-sponsored actors referred to as advanced persistent threats identified as having been conducting systematic hacking on a global scale to access intellectual property and sensitive data since 2014. With a huge explosion of multimedia big data including image, video, 3D, etc. literature suggests the rise of multi-modal challenges in relation to privacy [46]. Zhang et al. (2017) in fact propose an anti-piracy framework they term CyVOD to secure multimedia content copyrights against attacks [47].

Whilst historically espionage was limited to small scale operations with specific targets, [48] argues that the potential scale of espionage operations in cyberspace and their ability to impact the civilian population means that this level of ambiguity and uncertainty in international law can no longer be tolerated. [45] suggests the need for legal reforms are to adequately reflect the capabilities of modern technology. Furthermore, theory of expressive law [49] posits that these reforms influence state behaviour and identify underlying intolerance in society. In addition, one can conclude such reforms as critical for establishing new domestic laws to reduce the overall pervasiveness of espionage activities in cyberspace. With the overview of security challenges in cyberspace and the subsequent gaps and limitations the complexity of cyberspace imposed of a range of cyber strategies, the following subsection briefly explores how such gaps and limitations can be counteracted to enhance future cyber security operations.

2.1.1. Enhancing Cyber Security using Artificial Intelligence

To date, ongoing efforts focus towards soft computing and machine learning approaches to enhance computational intelligence [50]. In biology, several authors [51], [52], [53] and [54] to name a few, demonstrate the overwhelming use of machine learning approaches for predicting the survivability of cancer patients. While machine learning applications have been successfully applied in areas of science and computing security, remarkable growth of cyberspace, i.e. cloud computing, Internet of Things (IoT), web technologies, mobile computing, digital economy, etc. machine learning approaches have not been consistently applied. A few of the machine learning's core attributes; scalability, adaptability and the ability to adjust to new and unknown changes suggests them as suitable for application in cyberspace. For instance, handling and processing BigData or the capacity to perform computationally high calculations which were perhaps challenging in yesteryear are both significant opportunities machine learning presents. For cyber security, two main areas are a good fit for machine learning: 1. Data processing and 2. Expert systems.

The field of artificial intelligence (AI) has advanced faster than anticipated over the past five years [55]. Projects such as DeepMind's AlphaGo [56] is an example of funding commitments towards AI implementations. The application of AI to cyber operations is seen by [55] as a key milestone that has transformative implications for cyber security, enabling states to do more with fewer resources in a manner similar to the impact cyber operations had on the potential scale of intelligence operations. [57][58] [59] in fact identify five sub-fields of AI as possible areas to enhance both offensive and defensive cyber operations. Nonetheless, emerging consensus amongst researchers [57], [58] and [59] highlights the scale of implications introduced by AI. Thus, Allen

and Chan [55] urge responsible, sustainable and effective use of AI, including legal, ethical and economic concerns. The table below presents subfields of AI, their possible application as offensive and defensive security countermeasures.

Table 1-2. Examples of AI application as defensive and offensive countermeasure

AI Subfield	Possible cyber utility (defensive)	Possible cyber utility (offensive)
Expert systems	Identifying deceptive media	Producing deceptive media
Machine learning	Threat detection and future forecasting of attacks	Detection of opensource vulnerabilities; countermeasure evasion
Deep learning	Attack detection and malware identification	Brute forcing existing countermeasure, e.g. password
Computer vision	Predicting cyber-attacks, detecting and identifying vulnerabilities and generating patching solutions	Discover new sophisticated and zero-day attacks
Natural language processing	Anomaly detection and Botnet identification	Social engineering

2.3 Need for Unconventional Approaches to Cyber Security

The motivation for seeking inspiration from other systems is necessary due to the observation that cyberspace and inherently cyber security environments are complex. In other fields, for instance robotics, analogies to the immune system are exploited to design self-organisation mechanisms [12]. Biological concepts have been central and contributed to robust

implementations in a range of domains including computing, financial modelling [60] and robotics [61] to name a few. The underlying strengths of biological systems lies in their distributed architecture, where autonomous entities make local decisions with global implications [62]. For instance, the immune system is able adapt and self-protect by dynamically creating and destroying mutated or infected body cells, as it learns new threats and protects itself and its protective components [62]. As virtualization is commonplace in cyberspace, software defined platforms and networks rely heavily on it, however, security monitoring becomes harder as the attack surface is both new and wider [63]. Thus, the robustness of cyber technologies and infrastructures is determined by the quality of the underlying virtualization, while sophistication of technological resources influence the level of implementations [64].

Nature effectively demonstrates self-organization, adaptability, resilience and other successful phenomenon [65]. The strengths in natural systems resides in the ability of autonomous entities to make local decisions, continuously coordinate and share information, to maintaining a global form of order [18]. The predator-prey dynamic for instance, highlights the importance and consequences of interactions between two species and how the functions of a community depend on the characteristics of that community.

Biological systems have been a subject of research across the computing continuum stretching back to the 1980s [66]. In recent years, several surveys [67] [65] [68] [69][19], have dedicated their efforts towards evaluating biologically inspired algorithms in computing related applications. With the growth in demand on networked systems and reliance on internet connectivity provided through an assortment of devices and infrastructures [19], it is imperative that computing systems are adaptive, resilient, scalable and robust enough to withstand failure, and dynamic enough to cope with changes. Bio-inspired approaches are argued to provide consistency

in performance over a long period of time [61], and indeed have in common, the complexity attributes and the relative success of inter-networked environments [67]. For instance, the self-organizing (SO) attribute of bio-systems employed in wireless ad hoc networks means that, clustering routing nodes enhances the scalability of data forwarding protocols [19]. As such, the network is rendered robust and can adapt to frequent topological changes.

Other works elucidate the genius of nature by forwarding the argument that systems inspired by biology deliver significant results to enable exploration [70] and unique advances beyond the imagination of yesteryear [71]. This postulation is evident in performance optimization and enhancement of highly distributed and heterogeneous environments such as data centers, grids and clouds [72]. Nonetheless, as has been argued in literature, not all assumptions on biological algorithms are without limitations [73]. Despite the mentioned limitations, there remains undoubtedly huge potential in the use of bio-inspired methods as unconventional solutions to problems in the computing continuum. It is logical to be relatively optimistic considering how understanding physiological and ecological factors in biology has enabled medical innovation to cure and in some cases eradicate diseases [74].

Figure 4 is a taxonomic of example bio-inspired approaches distinguished according to their physiological and ecological attributes. Phenomenon such as the evolutionary implications of predation on adaption and counter-adaption, determine behaviors in species. Behaviors including predation risk and cost assessment in foraging species [75], change in response to outcomes of interactions between entities and their environment [76]..

Based upon interactions and behaviors that exist between a predator and its prey, a range of innovations have been developed. To this end, [77] applies the predator-prey dynamic; the principles of the cost of predation in particular, as a new approach for malware prevention. Similarly

[78] posits the predator-prey paradigm as the beneficial worm (predator) that terminates an intruding worm, and the malicious worm (prey) being the undesirable in a system. [79] work is grounded on the self-management attributes of a zebra herd against predators. [80] [81] aimed to resolve virus and worm challenges in distributed systems is based on attributes of successful predators found in predating communities. The authors in [82] explain that conventional security approaches focus on performing complex analysis on restricted datasets, whereas unconventional mechanisms process small amounts of data in a "simple distributed fashion" over a wide array of inputs. Many forms of biologically inspired artificial intelligence systems are shown to be successful when applied to an IDS, with Genetic Algorithms (GA) being particularly successful [83]. Despite their success, these approaches tend to improve on the efficiency of older techniques and many issues such as single-entry point analysis remain. When considering the defense of cloud systems against network aware malware, it is important to note that such systems now encompass multiple nodes based within complex network structures. Whilst conventional security defenses (single entry point analysis) are suitable for single machines, new unconventional defense systems are required to secure these complex networks. As such the application of distributed biological defense systems to computer networks would be more suitable to solve many problems, be it malicious software or others.

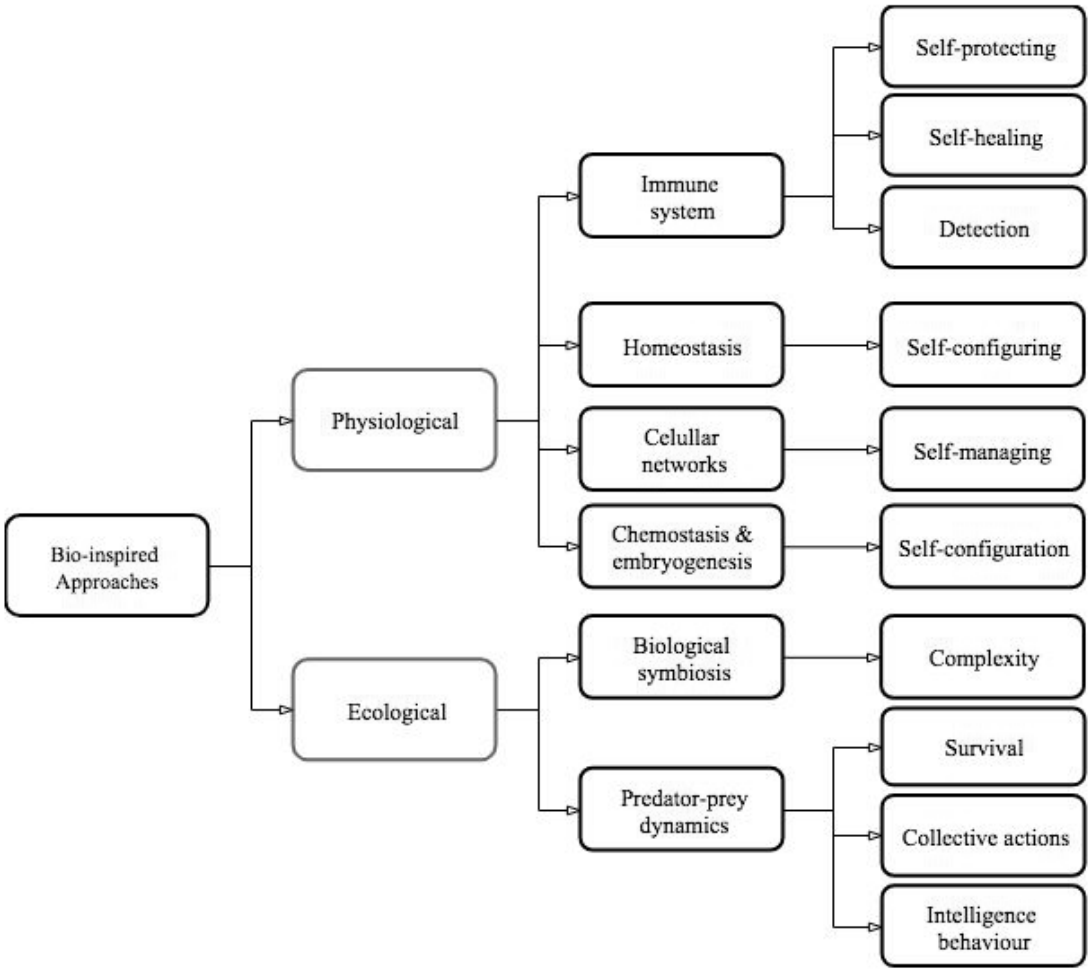

Figure 1- 4. A taxonomic example of bio-inspired approaches.

Bio-inspired approaches applied in traditional distributed computing systems demonstrate useful characteristics derived from their biological parentage; attributes which define origin, development, and progression, or ecological; interactional factors between organs and organisms in their natural environments. For instance, the design of IDSs based upon negative selection of T-cells that bind and kill infected or harmful cells [19]. Alternatively, the adaptation of the memory and self-learning mechanism employed by B-cells in identifying and destroying pathogens for designing IDSs [19] applies to physiological metaphors of the immune system. Given the significant success of biological systems, it seems logical to investigate theoretical underpinnings

that describe the core elements of this chapter, their application as plausible approaches in the cyber security continuum. To counteract insecurity, unconventional mechanisms and strategies of proactive defense, synonymous with those found in nature including deceptive strategies such as honeypots can be implemented as passive decoys against adversaries, or as active lures to distract adversaries [84]. Countermeasures have been suggested including aggressive approaches such as "white worms" [85] which actively pursues malicious software with an intent to destroy it. Deceptive techniques such as address hopping [86] protect data in transit by masking the actual visibility of a transmitting device from a possible attacker.

The following section investigates biological systems further, considering complexity and self-organisation in natural systems as possible fit for cyber security. Foremost, this section will present brief overview of common biological systems and their application areas. This will be followed by exploring existing applications on computing security in general followed by an evaluation of concepts' applicability in cyber security. In the subsequence subsections, the predator-prey dynamic; prey's predations avoidance and anti-predation mechanisms are speculatively applied as a cyber security case scenario. Predation avoidance is speculatively viewed as an exploitable mechanism to enable survivability in cyberspace. Previous works by [87]; [88][89] provide comprehensive reviews that contribute towards the unconventional context of the current section.

3. Review of Bio-inspired Methods

Among many works, the authors in [65] present a comprehensive survey of bio-inspired networking protocols, citing a substantial number of sources alluding to the fact that immune-inspired algorithms form the basis for network security; anomaly and misbehavior detection [65]. The authors associated epidemiology to content distribution in computer networks, including the

analysis of worms and virus spreading on the internet. The authors in [67] concur by associating intrusion detection and malware propagation with AIS and Epidemiology, respectively, as complimentary bio-inspired domains. In other works, the authors in [90] proposed a trust and reputations model (BTRM-WSN) inspired by the ant colony, as a strategy to leverage trust selection according to the most reputable path [92]. Although their model is designed for wireless sensor networks, it is reasonable to assume that, the underlying trust model can be extended to cloud computing environments by adapting the ant colony system [92] in which paths to fulfil defined conditions are built by leaving pheromones residues so that trailing ants can follow as a trusted route. Other models including the Trust Ant Colony System (TACS) [93], AntRep algorithm based on swam intelligence [94], Time Based Dynamic Trust Model (TBDTM) [95] to name a few, have been proposed for distributed systems. Nevertheless, it is imperative to emphasize the need for comprehensive testing and evaluation before their use in cloud environments [96].

Inspired by the reliability of gene identification and assignment inherent in biological systems, Wang et al. propose the Family-gene Based model for Cloud Trust (FBCT) to address existing limitations inherent in PKI-based systems, which include challenges in identifying nodes within cloud environments, access control, and third party authentication system [97]. According to the authors in [99], by adopting biological principles in family genes, their model provides solutions for trust in the cloud computing domain. Works by [79] explored the use to biological metaphors as a basis for designing, modelling and implementation of a cloud based web service, which is able to deal with counter stability issues that arise from long-running processes, and security attacks [79]. According to the authors, their proposed zebra herd-inspired approach not only simplified complex technical challenges, but also enhanced new designs for automated self-management processes for system administrators. Table 3 below summarizes some inspirational

bio-systems, categorizing them according to their application area, and the strengths and weaknesses of each system.

Faced with a combination of persistent and sophisticated adversaries, it is important that cyber security countermeasures are developed based on the foundations harvested from nature. Existing solutions simply fail as they do not adapt and escalate their security strategies to counteract the intensity and shear aggressiveness of an adversary [98]. [26] suggest security countermeasures as only successful in traditional networks. Thus, these authors postulate the rise in popularity of Adaptive Cyber Defense (ACD) approaches such as bio-inspired systems, based upon their ability to optimize unpredictability and maximize the adaptive configurations in attack surface, thereby raising the cost of an attack for the adversary [26]. Complexity, large-scale virtualization and the extremely distributed nature of the cyberspace means that accountability, auditability and trust in such ubiquitous environments becomes pivotal [99] [100].

Table 1-3. Summary of Bio-inspired approaches in cyber environments

Algorithm	Description	Application	Author
Multiple Sequence Alignment (MSA) algorithm	Protein structure	Web traffic classification & sequence alignment	[101]
IDS detector optimization algorithm with co-evolution	Co-evolution in populations	Optimizing IDS intrusion detection	[102]
Data Security strategy for	Immune systems	Stored data security	[103]

Secure Data Storage	Physiological & behavioral patterns	Biometric authentication cloud stored data	[104]
AIS for phishing Detection	T-lymphocytes life cycle	Phishing detection for emails	[105]
Integrated Circuit Metrics (ICMetrics)	Human properties & features	High entropy public/private key generation scheme	[106]
Biologically-inspired Resilience	Cells & organisms (sea chameleon)	Manages cloud security & leverage resilience	[98][107]
Data Hiding for Resource Sharing Based on DNA	DNA sequences	Data hiding for confidentiality & integrity of cloud data	[108]
Organic Resilience Approach for assuring resiliency against attacks and failure	Immunology (inflammation & immunization)	Threat detection, automated re-organization for assurance	[109]
Security based on Face Recognition	Facial features	Authentication and authorization	[110]
Family-gene Based model for Cloud Trust (FBCT)	Gene identification & assignment	User authentication, access control, & authorization	[111]

Agent of Network Danger Evaluation	Immune System:		[112]
Supervised learning classifier with real-time extraction (UCSSE)	Genetic-based machine learning	Adaptive & automatic signature discovery in IDS	[113]
Fraud detection & improper use of both computer system & mobile telecommunication operations	Immune System	Monitoring & detection of fraudulent intruders	[114]
Extension of Predator Prey Model	Predator-prey communities	Tackles automated mobile malware in networks	[80]
Computer Immune System	Innate immune phase	IDS mimics immune antigens to create signature strings	[115]
AntNet	Ant colony optimization algorithm & OS theory	Agents concurrently traverse a network and exchange information synonymous with stigmergy in insects.	[116]

Current examples of classic bio-inspired approaches in the computing continuum includes theories and algorithms. According to [66], algorithms are useful for describing systems with discrete state space, i.e. how and why systems transition occurs [66]. For instance, algorithms based on mechanisms governing the behaviors of ant colonies, human immune system, bees swarming, fish, predator and prey interactions and communities, etc. have been modelled to produce highly efficient, complex and distributed systems [71]. Prominent areas in computing where bio-inspired algorithms have been applied includes, but is not limited to, Autonomic computing [117], Artificial Life [118], Biomimetic [119], Organic Computing [120], and Genetic Algorithms [121]. In addition, theories such as the Self and Non-self, and Danger Theory [62], have been coined out with their primary premise on inspirations from biology. Further developments in bio-inspired approaches also necessitated the formalization of the Concurrency Theory as a formal framework for modelling parallel, distributed, and mobile systems [66]. In the ensuing subsection, we will highlight bio-inspired approaches applied in solving security issues in distributed and cloud computing systems. Bio-inspired approaches in this context imply mechanisms employed to facilitate and/or enhance the protection of data in distributed systems; as related to networked workstations and servers, the network itself including communication devices, etc. and cloud computing.

3.1 Bio-inspired Approaches

Artificial natural immune systems are applied in a variety of areas, and particularly lauded for its success in IDS [102]. Immune detectors determine the performance of the detection component of the immune system, a core component of the immune system [122]. Several works including [112] [115] [123] [124] to name a few, employ immune inspired approaches for

developing computer security mechanism based on the self-adaptive, self-learning, self-organizing, parallel processing, and distributed coordination attributes of AISs. In addition, the authors in [105] propose AIS phishing detection is inspired by part of the immune system's response mechanism to pathogens; immature T-lymphocytes life cycle. By generating memory detectors from a static training data set and immature detectors through mutation, the proposed system detects incoming phishing emails through memory detectors, while the immature detectors detect phishing emails with unknown signatures. Fang et al. posit the notion that their proposed systems performed well in phishing detection. Nonetheless, the authors contend to the fact that, using a static instead of dynamic fire-threshold value on their detectors, their system suffers from deficiencies [105]. Similarly, [125] explore the use of immune-inspired concept of apoptosis for in computer network security, which essentially describes the immune system's programmed action of destroying infected or mutated cells [125]. A comprehensive review of phishing email filtering techniques is presented by [126], while works by [127] reviews current literature and present a range of solutions proposed against identified attacks.

Genetic algorithms (GA) are stochastic search methods inspired from principles in biologicals systems where problem solving is indirect through an evolution of solutions, with subsequent generations of solutions in turn yielding the best solution to a problem [128]. Along similar lines, [129] proposed GTAP gene-inspired algorithm for user authentication where users from a "family" are identified by a unique gene certificate (synonymous with unique signatures), and users are authenticated upon a positive analysis of their gene code [129]. According to the authors, simulation results for GTAP demonstrated superiority in safety and security by countering the deficiencies in safety passwords and ambiguity of subject information in certificates presented in traditional mechanisms [129]. In other works [130], genetic algorithms are implemented in

cryptography to evaluate and enhance the complexities of encryption systems. An interested reader is referred to a complete guide for cryptographic solutions for computer and cyber security presented by [131]. In cryptanalysis, where an attack mechanism in implemented to assess the strength of an encryption system, GA are argued to be highly successful in substitution ciphers [132] and transposition ciphers [133]. Although neural networks are generally popular in pattern recognition and classification, and noise filtering, they are useful in other areas including the use of biometrics in security [128]. Key to their success is their accuracy in feature extraction and efficiency in classification, i.e. low rejection rate and high positive classification [128]. Along these lines, [134] proposed the Network Nervous System as a mechanism for effective protection against distributed denial of service (DDoS) attacks, grounded on the biological metaphor of the human central nervous systems; distributed information gathering and processing, coordination, and identification activities. Their work rests on the basis that traditional security tools fail to cope with the escalating power of attacks on computing infrastructures [134].

Ant colonies have been applied for routing traffic optimization, for instance in works by [116] who evaluate an optimization algorithm; AntNet, in which agents concurrently traverse a network and exchange information synonymous with stigmergy in insects. According to the authors, this algorithm exhibited superior performance in contrast to its competitors [135]. [136] proposed FBeeAd-Hoc as a security framework for routing problems in Mobile ad hoc networks (MANET) using fuzzy set theory and digital signature [136]. Works by [80] extends on previous work on the Predator model, to propose countermeasures against automated mobile malware in networks. The author proposes additional entities including immunization, persistent and seeking predators, modelled from the self-propagating, self-defending and mobility attributes found in predating animals as solutions to challenges mentioned above. Their works premises on the notion

that traditional countermeasures, which are generally centralized, fail adequately scale to solve security challenges existing in distributed systems [80]. According to the authors, their model does not only counter effects of malware attacks on a computer, but effectively distributes updates and patches to the infected computer, which in essence immunizes if from future attacks [80]. [137] suggest the use of predator models as inspirational solutions against viruses and worms.

3.2 Considerations Before Applying Bio-inspired Approaches

Before biological systems may be applied, there are several problems that should be considered. A panel discussing issues concerning biological security systems [82] describes a number of these. The first and perhaps most important is that biological systems and computer systems do not share an end goal. Whereas biological systems aspire to survive, the goal of many computer systems is to accomplish a computational task. This would serve to create doubt as to whether the model would remain effective when its goals were not the same. The authors [82] suggest that the survival of biological systems is an inherent issue within computer systems for the reason that, biological systems will perform sacrifices to achieve the goal of survival. Whereas in computer networks, downtime from a system is not something that is permitted, particularly if there is sensitive data that is to be protected. It is then argued that to achieve the characteristics wanted from biological systems (self-repair, organization, defense) then the whole system must be implemented, not just small sub-systems. This may be regarded as difficult if the systems may not be implemented properly due to contrasting goals. Nonetheless, it may be argued that software defined systems (SDS) maybe a useful link for integrating unconventional applications, platforms and infrastructures and managing them via APIs. Hence, developing cyber security solutions should consider the diversity of entities in cyberspace and the dynamic changes diversity brings, i.e.

requirement, goal, security, survivability, etc. Integrating self-awareness, self-adaptation, self-organization, to name a few, into cyberspace enables adaption to change at runtime.

4. Prey-inspired Survivability

Survivability in cyber environments as in nature is affected by a range of factors, including interactive high-order behaviours of both human factors and actors. Asymmetric warfare theory [138] makes the human factor/actor more apparent by alluding to time and stealth advantage attackers possess. The human factor/actor is demonstrated in the cyber context by the possibility for side-channel attackers to implant arbitrary code into a neighbour's VM environment with little to no chances of detection [139][140]. Considering the above, it is necessary to pose the question of how to best evaluate cyber infrastructure's survivability. This is a common challenge in complex and time-varying systems and requires methodological evaluations approaches that accommodate intermediary states that cyberspace resembles. As [141] suggest, the traditional binary view of survivability as ineffective in complex environments.

Clearly, the complexity of evaluating and later assuring survivability in cyber environments is a currently a challenging issue and requires a composite approach. There is an urgent need to combine traditional and complex formalisms to enhance secure deployment, provision and access to cyberspace systems. This chapter suggests drawing parallels between predation avoidance in animal communities and capabilities of security systems to survive compromise in cyberspace environments, in which the goal is to protect assets by hiding its visibility and increasing the complexity of being observed. By increasing the complexity of an asset, this adeptly increases the cost of an attack, increase the complexity of executing an exploit and gives an advantage to the defender [142]. In [143]'s model for instance, deceptive measures are employed to enhance

intelligence for the defender, while thwarting an adversary's capabilities to observe, investigate and learn about a target. Predator-prey systems (PPS) demonstrate complex relationships through interacting entities in which one depends on the other for food and survival [144]. Nevertheless, evidence in literature suggests that predator-prey models have found limited application in core cyber security domains including cloud computing security systems. Thus, predator-prey analogies can be developed to capture unique diversification mechanisms which ensure survivability in both homogeneous and heterogeneous prey species.

4.1 Anti-predation and Predation Avoidance Mechanisms for Cyber Security

The presence of a strong predation avoidance responses in nature's prey species demonstrates that past species interactions affect present distributions and may play an important role in the ongoing assembly of contemporary communities. Such avoidance behaviors in a growing number of species fundamentally alters our view of the processes affecting species distributions and the process of community assembly." [145]. In vervet monkey (*Cercopithecus aethiops*), vigilance is an anti-predator behavior shared between males and females, however much, with higher levels of vigilance is performed by males who spend more time on tree tops [146]. The importance of vigilance in vervet groups provides the best chances of survival by reducing the risk for individuals. On the other hand, consideration in group size effect, highlights an overall increase in vigilance in larger group sizes, and improved reaction to approaching predators. Furthermore, flight, alarm calls and response to alarm calls in vervet are adapted as responses to alarm calls associated with specific predator species [147]. As in fishes, alarm signals in vervet monkeys perform multiple-duties, ranging from predator deterrents, or distress signals to call in mobbers [148].

Social behaviors in Thomson's gazelles such as their alert posture, galloping, stotting, and soft alarm calls are argued to release alertness and flight information to avoid predation [149]. In some rare cases, adult Thomson gazelles (*Eudorcas Thomsonii)* will attempt to evade predators by lying down, yet in some instances, mothers are known to adopt aggressive defense strategies to divert predators from hunting their fawns [150] [149]. According to the authors, Thomson gazelles generally do not fight back predators when hunted [149]. As noted by [151], predation avoidance in Thompson gazelles is also associated with their grouping behaviours, i.e. larger groups have improved predator detection capabilities, and their vulnerability factor against their greatest predator; cheetah, (Acinonyx jubatus), significantly reduces in larger groups. Evidence in literature supports the claim that Stotting in Thompson gazelles is a vital tool for avoiding predation.

Evidence in literature supports the claim that stotting in Thompson gazelles is a vital tool for avoiding predation. Evidence include hypothesis which argue stotting to startle or confuse a predator, and as an anti-ambush evasion technique (Caro, T.M., 1986). Evidence in from Heinrich's (1979) works suggests at least five predation avoidance strategies employed by caterpillars (*Pyrrharctia Isabella*) against predating birds; restrict their feeding to underside of leaves, forage at night, use leaves for movement while foraging, distance themselves from an unfinished leaf, or snip it off altogether [152]. Like Vervet and Thomson's gazelle communities discussed above, group living is argued to positively enhance an individual's protection, as warning signals, defensive movement, and regurgitating noxious chemicals may increase survivability [153]. Indeed, this is true considering the activities males in vervet communities, who take up high positions on tree tops to scan their surroundings and raise alarms when they detect predation threats. Thus, males are functionally associated with observation, vigilance, and are perceived as most active against predators [146].

The choice of predation avoidance or anti-predation mechanism is hugely important in Meerkat (*Suricata suricatta*) communities as they live under high predation pressures, while occupying challenging foraging niche [154]. As such, social learning (developed and molded by experience), and effective cooperation initiate key survival behaviors, including fleeing non-specific predators, mobbing against predating snakes, functional referential alarm calls, or running to bolts holes in response to aerial predators [154]. In addition, Meerkat depend hugely on group living through communal vigilance [155] which unlike response to alarm calls avoids imminent predation, vigilance occurs in the absence or presence of a predator or danger [156]. Zebras' fleeing responses to predating lions are described according to their proactive responses to a prior assessed risk level and reactive responses when predation is imminent [157]. According to the authors, responses against predation also extended to elusive behaviors, where zebra remove themselves as far away from an encounter habitat (usually waterholes) as possible. In contrast to animal prey, plant prey significantly their predation cost to potential predators as the handling time and processing of plant tissue is more taxing. In the following, the current section will focus upon five successful prey species, to explore survival mechanisms. Vigilance, alarm calls, mobbing and group living are anti-predator behaviours shared among vervet monkeys (*Cercopithecus aethiops*). Within this community, Vervet males are associated with higher levels of vigilance [146]. Vigilance in larger groups increases, which improves reaction to approaching predators. Furthermore, flight and response in vervets is adapted to alarm calls associated with specific predator species [147]. Survival techniques employed by prey entities include changes in functioning, behaviours, and structure, enabling them to avoid detection and hence predation. The foregoing is summarised in Table 4 where survival mechanisms for each natural community is distinguished as either a predation avoidance behaviour or an anti-predator technic. Predation avoidance and anti-predation

mechanisms describe the main objectives of diversification, which in turn define how prey species behave to improve selection and survivability [158]. Anti-predation mechanisms describe prey techniques which reduce the probability of predation, while predation avoidance describes mechanism prey uses to remove itself from the same habitat as the predator.

Table 1-4. Examples of prey survival mechanisms

	Survival mechanism/ behaviour	**Plants**	**Flat-tail horned lizard**	**Vervets**	**Thomson gazelles**	**Moth caterpillar**	**Meerkat**	**Equus quagga (Zebra)**
Anti-predation	Alarm calling	×	×	✓	✓	×	✓	✓
	Chemical-def	✓	×	×	×	×	×	×
	Fight-back	✓	✓	✓	×	✓	✓	✓
	Stotting	×	×	×	✓	×	×	×
	Group living	✓	×	✓	✓	✓	✓	✓
	Mobbing	×	×	✓	×	×	✓	×
	Aposematic	✓	×	×	×	✓	×	✓
	Mimicry	✓	✓	×	×	✓	×	×
Predation avoidance	Camouflaging	✓	✓	×	✓	✓	×	✓
	Masquerade	✓	✓	×	×	✓	✓	✓

Based upon the above, it is possible to develop analogies to capture unique diversification mechanisms that ensure survival in both homogeneous and heterogeneous prey species. Both

mechanisms (predation avoidance and anti-predation) describe the main objectives of diversification, which define how prey species behave in order to improve selection and survivability [158]. As killing of prey by predators is a focus of mathematical modelling as it is easily observable, [159] suggests anti-predation behaviours as most critical to prey survival.

Mechanisms for cyber security and cyber environments would thus consider both, the subjective and objective selection of anti-predator and predation avoidance mechanisms (techniques and behaviours). Mechanisms may exist as specific (where mechanisms are effective against a specific predator), or non-specific (where strategies are effective against all predators) [160]. Exploiting prey survival attributes as a blueprint for designing processes and mechanisms for cyberspace offers several benefits.

- Survivable preys possess unique attributes that are well adapted to their environments. One may conceptualise the design of cyber agents capable of escaping and/or counter-attacking a "predator". [161]'s mathematical formulations illustrate this efficacy.
- Survivable prey species possess strong and successful mechanisms that demonstrate the far-reaching implications historical interactions have on future species [145]. By understanding such mechanisms, it is possible to adopt/adapt such processes for future cyber security.
- Prey analogies that characterised non-extinct prey can be developed. [79] explored the use to biological metaphors for designing, modelling and implementing a web services capable of counteracting stability issues that arise from long-running processes and security attacks. Moreover, cloud computing, itself a core element of

cyberspace, is a metaphor for the internet [162] where services are provided as metered resources in electricity-like manner [163]

- Developing analogies from nature requires methodological approaches to translate apt prey functions for to cyber security environments [89]. This requires an understanding of relationships between the complexity of prey systems and their local stability; Theoretical Ecology [164] provides in-depth knowledge in this domain. Moreover, complexity theory [165] provides basis to deconstruct the complexity of cyberspace and nature systems.

5. Research directions in **Survivability Assurance in Cyberspace**

Recent trends towards bio-inspired designs have ushered the development of methods for creating analogies to combine attributes or objectives in multi-domain systems can in a formal manner [166]. BioTRIZ [167][168] and other analogical reasoning tools summarised in the table below are some common examples. While conceptual design (CD) provides insights into the functions, working principles and a general layout of a system's structure [169] they are deficient since a one-to-one transfer of nature concepts to cloud computing requires lateral thinking.

On the other hand, TRIZ (the Theory of inventive problem solving) is a useful systematic methodology that provides logical approaches for innovative and inventive creations [170]. TRIZ has been adapted to suit other environments such as information technology [171]. To capture key characteristics from nature , this paper follows Beckmann's approach [172], but specifically focus upon cloud computing rather than information technology in general. Since the original TRIZ principles provides abstract solution models [172], any new labels (we term prey-centric and cloud-

centric) are also abstract. Hence, any further developments generate further minute abstract solutions.

As postulated by [172], abstraction means that TRIZ principles are applicable in a wide range of fields. TRIZ provides the added capacity to identify a solution [172], whereupon conceptual solutions can further be developed into specific factual solutions. Indeed, conceptualising solutions is informed by identified specific problems, which in turn informs the choice of the problem-solving approach and tool

Table 1-5. Comparison of analogy development methods

Design Method	Description	Is knowledge of bio-system required?
Functional Modeling	Well defined categories and scale to develop functional models	Yes
BioTRIZ	Allows invention to solve problems with contradiction	No
BID Lab Search Tool	Natural language processing tool to search bio-words using engineering words	No
Biology Thesaurus	Extensible to a range of tools other than functional methods	Undefined
IDEA-INSPIRE & DANE	Provides organised database for bio-design	Undefined

Existing analogical design approaches rely largely on thematic mapping processes and subjective choices of the components of a biological system or sub-systems. For instance, by focusing upon the impact of ecological diversification [173], population dynamics [174], or simple constructs of an arms race [175]. This suggests the wrong notion that analogical design requires comprehensive understanding of cyber security technologies, but just the basics of the arms race [176]. In fact, as [177] argues, the designer's knowledge of both domains helps to infer information that facilitates bio-inspired designs from a problem or solution-driven perspective. Hence, the concept of analogies mentioned in this chapter proffer that, given an old problem (P_{old}) i.e. predate-survive dynamic, with an old solutions (S_{old}) i.e. predation avoidance and antipredation, a new problem (P_{new}) i.e. cyberspace survivability can be conceptualized with new partial and perhaps null solutions (S_{new}) i.e. prey-inspired predation avoidance analogies in the solutions space Sold to S_{new}.

Designing cyber security solutions should consider the diversity of entities, and the dynamic changes diversity brings, i.e. requirement, goal, security, survivability, etc. Integrating self-awareness, self-adaptation, self-organization, to name a few, into cloud environment design enables service composition to adapt to changes at runtime. On one hand, underlying designs cannot be static and inadequate for synthesizing dynamic and distributed service compositions. On the contrary, designs should enable distributed coordination of entities necessary to achieve agreeable levels of survivability. In addition to integrating the three-selves (self-aware, self-configure, self-organize), automation supports necessary adaptation. At design time for instance, holistic synthesis of the cloud logic entails automated and fully distributed coordination of the involved entities and services. During execution, automation facilitates adaptation through "self-attributes" synthesizing dynamically evolving entities. Multi-agent-based systems are lauded for complex behaviours

among interacting autonomous agents. By extending multi-agent capabilities into cyber environments, challenges including security, survivability and availability can be better managed. As suggested by [178], integrating multi-agent technologies can unlock even higher performing, complex, autonomous and intelligent applications and scalable yet reliable infrastructures.

7. References

[1] D. J. Betz and T. Stevens, "Analogical reasoning and cyber security," *Secur. Dialogue*, vol. 44, no. 2, pp. 147–164, 2013.

[2] And, "TOWARDS A MORE REPRESENTATIVE DEFINITION OF CYBER SECURITY," pp. 53–75.

[3] A. Klimburg, *National Cyber Security Framework Manual*. 2012.

[4] BBC online UK, "Vodafone Germany hack hits two million customers," *BBC*. [Online]. Available: https://www.bbc.co.uk/news/technology-24063621. [Accessed: 10-Jun-2018].

[5] BBC online UK, "TalkTalk hack 'affected 157,000 customers,'" *BBC*, 2015. [Online]. Available: https://www.bbc.co.uk/news/business-34743185. [Accessed: 10-Jun-2018].

[6] BBC online UK, "Dixons Carphone admits huge data breach," *BBC*, 2018. [Online]. Available: https://www.bbc.co.uk/news/business-44465331. [Accessed: 13-Jun-2018].

[7] A. Ghoneim, G. Muhammad, S. U. Amin, and B. Gupta, "Medical Image Forgery Detection for Smart Healthcare," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 33–37, 2018.

[8] Iso Iec, "BS ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management," *ISO*. p. 130, 2005.

[9] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[10] R. Foote, "Mathematics and complex systems," *Science*, vol. 318, no. 5849. pp. 410–412,

2007.

[11] G. Wen, W. Yu, X. Yu, and J. Lü, "Complex cyber-physical networks: From cybersecurity to security control," *J. Syst. Sci. Complex.*, vol. 30, no. 1, pp. 46–67, 2017.

[12] F. A. C. Polack, "Self-organisation for survival in complex computer architectures," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6090 LNCS, pp. 66–83, 2010.

[13] O. Vermesan and P. Friess, *Internet of Things Applications - From Research and Innovation to Market Deployment*. 2014.

[14] S. Alam, I. Sogukpinar, I. Traore, and Y. Coady, "In-Cloud Malware Analysis and Detection : State of the Art," *Proc. 7th Int. Conf. Secur. Inf. Networks - SIN '14*, pp. 473–478, 2014.

[15] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[16] Tewari, A. and Gupta, B.B., "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices," *Int. J. Adv. Intell. Paradig.*, vol. 9, no. 2–3, p. pp.111-121, 2017.

[17] J. T. Hoverman and R. A. Relyea, "Survival trade-offs associated with inducible defences in snails: The roles of multiple predators and developmental plasticity," *Funct. Ecol.*, vol. 23, no. 6, pp. 1179–1188, 2009.

[18] A. H. Sayed, "Adaptive networks," *Proc. IEEE*, vol. 102, no. 4, pp. 460–497, 2014.

[19] C. Zheng and D. C. Sicker, "A survey on biologically inspired algorithms for computer networking," *Commun. Surv. Tutorials, IEEE*, vol. 15, no. 3, pp. 1160–1191, 2013.

[20] C. L. Smith, "FUNDAMENTALS OF CONTROL THEORY.," *Chemical Engineering (New York)*, vol. 86, no. 22. pp. 11–39, 1979.

[21] I. D. Landau, "From robust control to adaptive control," *Control Eng. Pract.*, vol. 7, pp. 1113–1124, 1999.

[22] J. Andersson, R. De Lemos, S. Malek, and D. Weyns, "Modeling dimensions of self-adaptive software systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5525 LNCS, pp. 27–47.

[23] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[24] K. Hausken and F. He, "On the Effectiveness of Security Countermeasures for Critical Infrastructures," *Risk Anal.*, vol. 36, no. 4, pp. 711–726, 2016.

[25] P. Checkland, *Systems Thinking, System practice.* 1981.

[26] G. Cybenko, S. Jajodia, M. P. Wellman, and P. Liu, "Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundation," Springer, 2014, pp. 1–8.

[27] N. Virvilis and D. Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, 2013, pp. 248–254.

[28] R. J. Harknett and J. A. Stever, "The New Policy World of Cybersecurity," *Public Adm. Rev.*, vol. 71, no. 3, pp. 455–460, 2011.

[29] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[30] C. A., "The Eight Providers That Matter Most and How They Stack Up." The Forrester

WaveTM, 2016.

[31] N. Shahriar, R. Ahmed, S. R. Chowdhury, A. Khan, R. Boutaba, and J. Mitra, "Generalized recovery from node failure in virtual network embedding," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 2, pp. 261–274, 2017.

[32] S. Ren *et al.*, "A coordination model for improving software system attack-tolerance and survivability in open hostile environments," *Int. J. Adapt. Resilient Auton. Syst.*, vol. 3, no. 2, pp. 175–199, 2013.

[33] H. Baheti, R. and Gill, "Cyber-physical systems. The impact of control technology," 2011, pp. 161–6.

[34] HM Government, *A Strong Britain in an Age of Uncertainty : The National Security Strategy*, vol. 16, no. Supplement. 2010.

[35] Joint Committee on the National Security Strategy, "National Security Strategy and Strategic Defence and Security Review 2015," *First Rep. Sess. 2016-17*, vol. HL Paper 1, no. HC 153, pp. 1–96, 2016.

[36] M. Mount and E. Quijano, "Iraqi insurgents hacked Predator drone feeds, U.S. official indicates," *CNN*, 2009. [Online]. Available: http://www.cnn.com/2009/US/12/17/drone.video.hacked/.

[37] R. Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *Arlington, VA Langner Gr.*, no. November, pp. 1–36, 2013.

[38] Y. Ryan, "Anonymous and the Arab uprisings," *Aljazeera.com*, pp. 1–5, 2011.

[39] A. Segal, "Net {Politics} » {The} {UN}'s {Group} of {Governmental} {Experts} on {Cybersecurity}," *Council on Foreign Relations - Net Politics*. 2015.

[40] R. Hurwitz, "Depleted trust in the cyber commons," *Strateg. Stud. Q. VO - 6*, no. 3, p. 20,

2012.

[41] D. P. Fidler, "Cyberspace, terrorism and international law," *J. Confl. Secur. Law*, vol. 21, no. 3, pp. 475–493, 2016.

[42] United States Defense Force, "Joint Publication 3-12 Cyberspace Operations," *United States Def. Force*, vol. 12, no. February 2013, p. 62, 2013.

[43] D. Pun, "Rethinking Espionage in the Modern Era," *Chic. J. Int. Law*, vol. 18, no. 1, 2017.

[44] E. Osnos, D. Remnick, and J. Yaffa, "Trump, Putin, and the New Cold War," *new yorker*, no. 1, pp. 1–77, 2017.

[45] PwC and BAE, "Operation Cloud Hopper," *PwC Web Site*. 2017.

[46] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in Security and Privacy of Multimedia Big Data in Mobile and Cloud Computing," *Multimed. Tools Appl.*, 2017.

[47] B. B. Zhang, Z., Sun, R., Zhao, C., Wang, J., Chang, C.K. and Gupta, "CyVOD: a novel trinity multimedia social network scheme.," in *Multimedia Tools and Applications*, 2017, p. pp.18513-18529.

[48] A. Deeks, "Confronting and Adapting: Intelligence Agencies and International Law," *SSRN Electron. J.*, 2016.

[49] R. Cooter, "Expressive Law And Economics," *J. Legal Stud.*, vol. 27, no. S2, pp. 585–607, 1998.

[50] S. Greibach, *Lecture Notes in Computer Science*. 2010.

[51] G. D. Magoulas and A. Prentza, "Machine Learning in Medical Applications," in *Machine Learning and Its Applications: Advanced Lectures*, 2001, pp. 300–307.

[52] D. Delen, G. Walker, and a Kadam, "Predicting breast cancer survivability: A comparison of three data mining methods," *Artif. Intell. Med.*, vol. 34, no. 2, pp. 113–127, 2005.

[53] K. Kourou, T. Exarchos, K. Exarchos, M. Karamouzis, and D. Fotiadis, "Machine Learning Applications in Cancer Prognosis and Prediction," *Computational and Structural Biotechnology Journal*, vol. 13. pp. 8–17, 2015.

[54] N. Shukla, M. Hagenbuchner, K. T. Win, and J. Yang, "Breast cancer data analysis for survivability studies and prediction," *Comput. Methods Programs Biomed.*, vol. 155, pp. 199–208, 2018.

[55] G. Allen and T. Chan, "Artificial Intelligence and National Security," *Belfer Cent. Sci. Int. Aff.*, 2017.

[56] D. Silver *et al.*, "Mastering the game of Go without human knowledge," *Nature*, vol. 550, no. 7676, pp. 354–359, 2017.

[57] E. Tyugu, "Artificial intelligence in cyber defense," *2011 3rd Int. Conf. Cyber Confl.*, pp. 1–11, 2011.

[58] P. Patil, "Artificial Intelligence in Cyber Security," *Int. J. Res. Comput. Appl. Robot.*, vol. 4, no. 5, pp. 1–5, 2016.

[59] B. Hallaq, T. Somer, A.-M. Osula, K. Ngo, and T. Mitchener-Nissen, "Artificial intelligence within the military domain and cyber warfare," *Eur. Conf. Inf. Warf. Secur. ECCWS*, pp. 153–157, 2017.

[60] A. Brabazon and M. O'Neill, *Biologically inspired algorithms for financial modelling*. Springer Science & Business Media, 2006.

[61] R. Oates, M. Milford, G. Wyeth, G. Kendall, and J. M. Garibaldi, "The implementation of a novel, bio-inspired, robotic security system," in *Robotics and Automation, 2009. ICRA'09. IEEE International Conference on*, 2009, pp. 1875–1880.

[62] T. S. Sobh and W. M. Mostafa, "A cooperative immunological approach for detecting

network anomaly," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 1275–1283, 2011.

[63] N. Ziring, "The Future of Cyber Operations and Defense," *Warfare*, vol. 14, pp. 1–7, 2015.

[64] C. Low, Y. Chen, and M. Wu, "Understanding the determinants of cloud computing adoption," *Ind. Manag. Data Syst.*, vol. 111, no. 7, pp. 1006–1023, 2011.

[65] F. Dressler and O. B. Akan, "A survey on bio-inspired networking," *Comput. Networks*, vol. 54, no. 6, pp. 881–900, 2010.

[66] C. Priami, "Algorithmic systems biology," *Commun. ACM*, vol. 52, no. 5, pp. 80–88, 2009.

[67] M. Meisel, V. Pappas, and L. Zhang, "A taxonomy of biologically inspired research in computer networking," *Comput. Networks*, vol. 54, no. 6, pp. 901–916, 2010.

[68] T. Nakano, "Biologically inspired network systems: a review and future prospects," *Syst. Man, Cybern. Part C Appl. Rev. IEEE Trans.*, vol. 41, no. 5, pp. 630–643, 2011.

[69] C. C. Ribeiro and P. Hansen, *Essays and surveys in metaheuristics*, vol. 15. Springer Science & Business Media, 2012.

[70] S. Thakoor, "Bio-inspired engineering of exploration systems," *J. Sp. Mission Archit.*, vol. 2, no. 1, pp. 49–79, 2000.

[71] M. Hinchey and R. Sterritt, "99% (Biological) inspiration," in *Conquering Complexity*, 2012, pp. 177–190.

[72] N. Wakamiya and M. Murata, "Bio-inspired analysis of symbiotic networks," Springer, 2007, pp. 204–213.

[73] M. Breza and J. McCann, "Lessons in implementing bio-inspired algorithms on wireless sensor networks," in *Adaptive Hardware and Systems, 2008. AHS'08. NASA/ESA Conference on*, 2008, pp. 271–276.

[74] S. B. Levy and B. Marshall, "Antibacterial resistance worldwide: causes, challenges and

responses," *Nat. Med.*, vol. 10, pp. S122–S129, 2004.

[75] A. D. Higginson and G. D. Ruxton, "Foraging mode switching: the importance of prey distribution and foraging currency," *Anim. Behav.*, vol. 105, pp. 121–137, 2015.

[76] N. DiRienzo, J. N. Pruitt, and A. V Hedrick, "The combined behavioural tendencies of predator and prey mediate the outcome of their interaction," *Anim. Behav.*, vol. 86, no. 2, pp. 317–322, 2013.

[77] R. Ford, M. Bush, and A. Bulatov, "Predation and the cost of replication: New approaches to malware prevention?," *Comput. Secur.*, vol. 25, no. 4, pp. 257–264, 2006.

[78] S. Tanachaiwiwat and A. Helmy, "Encounter-based worms: Analysis and defense," *Ad Hoc Networks*, vol. 7, no. 7, pp. 1414–1430, 2009.

[79] J. Finstadsveen and K. Begnum, "What a webserver can learn from a zebra and what we learned in the process," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, 2011, p. 5.

[80] A. Gupta and D. C. DuVarney, "Using predators to combat worms and viruses: A simulation-based study," in *Computer Security Applications Conference, 2004. 20th Annual*, 2004, pp. 116–125.

[81] H. Toyoizumi and A. Kara, "Predators: Good will mobile codes combat against computer viruses," in *Proceedings of the 2002 workshop on New security paradigms*, 2002, pp. 11–17.

[82] A. Somayaji, M. Locasto, and J. Feyereisl, "Panel : The Future of Biologically-Inspired Security : Is There Anything Left to Learn?," in *NSPW'07, September 18-21, 2007, North Conway, NH, USA*, 2007, pp. 49–54.

[83] G. Sakellari and G. Loukas, "A survey of mathematical models, simulation approaches and

testbeds used for research in cloud computing," *S.I.Energy Effic. grids clouds*, vol. 39, no. 0, pp. 92–103, 2013.

[84] C. F. L. López, M.H. and Reséndez, "Honeypots: basic concepts, classification and educational use as resources in information security education and courses," 2008.

[85] W. Lu, S. Xu, and X. Yi, "Optimizing active cyber defense," Springer, 2013, pp. 206–225.

[86] L. Shi, C. Jia, S. L, and Z. Liu, "Port and address hopping for active cyber-defense," Springer, 2007, pp. 295–300.

[87] S. N. Mthunzi and E. Benkhelifa, "Trends towards Bio-Inspired Security Countermeasures for Cloud Environments," in *Proceedings - 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems, FAS*W 2017*, 2017, pp. 341–347.

[88] T. Welsh and E. Benkhelifa, "Perspectives on resilience in cloud computing: Review and trends," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2017–Octob, pp. 696–703, 2018.

[89] S. Mthunzi and E. Benkhelifa, "Mimicking Prey ' s Escalation Predation-avoidance Techniques for Cloud Computing Survivability using Fuzzy Cognitive Map," pp. 189–196, 2018.

[90] F. G. Mármol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," *Comput. Secur.*, vol. 28, no. 7, pp. 545–556, 2009.

[91] D. H. Dang and J. Cabot, "Automating inference of OCL business rules from user scenarios," in *Proceedings - Asia-Pacific Software Engineering Conference, APSEC*, 2013, vol. 1, no. 4, pp. 156–163.

[92] M. Dorigo and L. M. Gambardella, "Ant colony system: a cooperative learning approach to the traveling salesman problem," *Evol. Comput. IEEE Trans.*, vol. 1, no. 1, pp. 53–66, 1997.

[93] F. G. Marmol, G. M. Perez, and A. F. G. Skarmeta, "TACS, a trust model for P2P networks," *Wirel. Pers. Commun.*, vol. 51, no. 1, pp. 153–164, 2009.

[94] W. Wang, G. Zeng, and L. Yuan, "Ant-based reputation evidence distribution in P2P networks," in *Grid and Cooperative Computing, 2006. GCC 2006. Fifth International Conference*, 2006, pp. 129–132.

[95] T. Zhuo, L. Zhengding, and L. Kai, "Time-based dynamic trust model using ant colony algorithm," *Wuhan Univ. J. Nat. Sci.*, vol. 11, no. 6, pp. 1462–1466, 2006.

[96] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing: A Critical Review," *Int. J. Adv. ICT Emerg. Reg.*, vol. 4, no. 2, pp. 24–36, 2012.

[97] T. Wang, B. Ye, Y. Li, and Y. Yang, "Family gene based Cloud Trust model," in *ICENT 2010 - 2010 International Conference on Educational and Network Technology*, 2010, pp. 540–544.

[98] S. Hariri, M. Eltoweissy, and Y. Al-Nashif, "Biorac: biologically inspired resilient autonomic cloud," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, 2011, p. 80.

[99] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Secur. Priv.*, no. 6, pp. 24–31, 2010.

[100] R. K. L. Ko *et al.*, "TrustCloud: A framework for accountability and trust in cloud computing," in *Services (SERVICES), 2011 IEEE World Congress on*, 2011, pp. 584–588.

[101] G. He, M. Yang, J. Luo, and X. Gu, "A novel application classification attack against Tor," *Concurr. Comput. Pract. Exp.*, vol. 27, no. 18, pp. 5640–5661, 2015.

[102] X. Liang and Z. Fengbin, "Detector optimization algorithm with co-evolution in immunity-based intrusion detection system," in *Measurement, Information and Control (ICMIC),*

2013 International Conference on, 2013, vol. 1, pp. 620–623.

[103] C. Jinyin and Y. Dongyong, "Data security strategy based on artificial immune algorithm for cloud computing," *Appl.Math*, vol. 7, no. 1L, pp. 149–153, 2013.

[104] K. Govinda and G. Kumar, "T SECURE DATA STORAGE IN CLOUD ENVIRONMENT USING FINGERPRINT," *ASIAN J. Comput. Sci. Inf. Technol.*, vol. 2, no. 5, 2013.

[105] X. Fang, N. Koceja, J. Zhan, G. Dozier, and D. Dipankar, "An artificial immune system for phishing detection," in *Evolutionary Computation (CEC), 2012 IEEE Congress on*, 2012, pp. 1–7.

[106] R. Tahir, H. Hu, D. Gu, K. McDonald-Maier, and G. Howells, "A scheme for the generation of strong cryptographic key pairs based on ICMetrics," in *Internet Technology And Secured Transactions, 2012 International Conference for*, 2012, pp. 168–174.

[107] T. Welsh and E. Benkhelifa, "Embyronic Model for Highly Resilient PaaS," pp. 197–204, 2018.

[108] M. R. Abbasy and B. Shanmugam, "Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences," in *Services (SERVICES), 2011 IEEE World Congress on*, 2011, pp. 385–390.

[109] M. Carvalho, D. Dasgupta, M. Grimaila, and C. Perez, "Mission resilience in cloud computing: A biologically inspired approach," in *6th International Conference on Information Warfare and Security*, 2011, pp. 42–52.

[110] C. Wang and H. Yan, "Study of cloud computing security based on private face recognition," in *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, 2010, pp. 1–5.

[111] T. Wang, B. Ye, Y. Li, and Y. Yang, "Family gene based cloud trust model," in *Educational*

and Network Technology (ICENT), 2010 International Conference on, 2010, pp. 540–544.

[112] J. Yang, X. Liu, T. Li, G. Liang, and S. Liu, "Distributed agents model for intrusion detection based on AIS," *Knowledge-Based Syst.*, vol. 22, no. 2, pp. 115–119, 2009.

[113] K. Shafi and H. A. Abbass, "An adaptive genetic-based signature learning system for intrusion detection," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 12036–12043, 2009.

[114] A. Boukerche, K. R. L. Juca, J. B. Sobral, and M. S. M. A. Notare, "An artificial immune based intrusion detection model for computer and telecommunication systems," *Parallel Comput.*, vol. 30, no. 5, pp. 629–646, 2004.

[115] J. O. Kephart, "A biologically inspired immune system for computers," in *Artificial Life IV: proceedings of the fourth international workshop on the synthesis and simulation of living systems*, 1994, pp. 130–139.

[116] B. Baran and R. Sosa, "A new approach for AntNet routing," in *Computer Communications and Networks, 2000. Proceedings. Ninth International Conference on*, 2000, pp. 303–308.

[117] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer (Long. Beach. Calif).*, vol. 36, no. 1, pp. 41–50, 2003.

[118] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune system architecture for computer security applications," *Evol. Comput. IEEE Trans.*, vol. 6, no. 3, pp. 252–280, 2002.

[119] B. T. OGRAPH and Y. R. MORGENS, "Cloud computing," *Commun. ACM*, vol. 51, no. 7, 2008.

[120] H. Schmeck, "Organic computing-a new vision for distributed embedded systems," in *Object-Oriented Real-Time Distributed Computing, 2005. ISORC 2005. Eighth IEEE International Symposium on*, 2005, pp. 201–203.

[121] L. Agostinho, G. Feliciano, L. Olivi, E. Cardozo, and E. Guimarães, "A bio-inspired approach to provisioning of virtual resources in federated clouds," in *Proceedings - IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC 2011*, 2011, pp. 598–604.

[122] Z. Ji and D. Dasgupta, "V-detector: An efficient negative selection algorithm with 'probably adequate' detector coverage," *Inf. Sci. (Ny).*, vol. 179, no. 10, pp. 1390–1406, 2009.

[123] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection - A review," *Natural Computing*, vol. 6, no. 4. pp. 413–466, 2007.

[124] F. A. Gonzalez and D. Dasgupta, "Anomaly Detection Using Real-Valued Negative Selection," *Genet. Program. Evolvable Mach.*, vol. 4, no. 4, pp. 383–403, 2003.

[125] M. M. Saudi, M. Woodward, A. J. Cullen, and H. M. Noor, "An overview of apoptosis for computer security," in *Information Technology, 2008. ITSim 2008. International Symposium on*, 2008, vol. 4, pp. 1–6.

[126] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013.

[127] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, 2017.

[128] W. Hordijk, "An Overview of Biologically Inspired Computing in Information Security," in *Proceedings of the National Conference on Information Security, Coimbatore, India*, 2005, pp. 1–14.

[129] F. Sun and S. Cheng, "A gene technology inspired paradigm for user authentication," in

Bioinformatics and Biomedical Engineering, 2009. ICBBE 2009. 3rd International Conference on, 2009, pp. 1–3.

[130] P. Isasi and J. C. Hernandez, "Introduction to the applications of evolutionary computation in computer security and cryptography," *Comput. Intell.*, vol. 20, no. 3, pp. 445–449, 2004.

[131] S. eds. Gupta, B., Agrawal, D.P. and Yamaguchi, *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI Global, 2016.

[132] A. K. Verma, M. Dave, and R. C. Joshi, "Genetic algorithm and tabu search attack on the mono-alphabetic substitution cipher i adhoc networks," in *Journal of Computer science*, 2007.

[133] R. Toemeh and S. Arumugam, "Breaking Transposition Cipher with Genetic Algorithm," *Elektron. ir Elektrotechnika*, vol. 79, no. 7, pp. 75–78, 2015.

[134] A. Shorov and I. Kotenko, "The Framework for Simulation of Bioinspired Security Mechanisms against Network Infrastructure Attacks," *Sci. World J.*, vol. 2014, 2014.

[135] G. Di Caro and M. Dorigo, "AntNet: Distributed stigmergetic control for communications networks," *J. Artif. Intell. Res.*, pp. 317–365, 1998.

[136] M. K. Rafsanjani and H. Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs," *AEU-International J. Electron. Commun.*, vol. 69, no. 11, pp. 1613–1621, 2015.

[137] R. Grimes, *Malicious mobile code: Virus protection for Windows*. " O'Reilly Media, Inc.," 2001.

[138] R. Baskerville, "Agile Security for Information Warfare: A Call for Research," *ECIS 2004 Proc.*, p. 10, 2004.

[139] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud:

exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 199–212.

[140] S. N. Mthunzi, E. Benkhelifa, M. A. Alsmirat, and Y. Jararweh, "Analysis of VM Communication for VM-based Cloud Security Systems *," pp. 182–188, 2018.

[141] Q. Liang and E. Modiano, "Survivability in Time-Varying Networks," *IEEE Trans. Mob. Comput.*, vol. 16, no. 9, pp. 2668–2681, 2017.

[142] M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in *Proceedings of the 2nd conference on Human System Interactions, HSI*, 2009, vol. 9.

[143] J. Yuill, D. E. Denning, and F. Feer, "No Title," *Using Decept. to hide things from hackers Process. Princ. Tech.*, 2006.

[144] M. A. Colomer, A. Margalida, D. Sanuy, and M. J. Perez-Jimenez, "A bio-inspired computing model as a new tool for modeling ecosystems: the avian scavengers as a case study," *Ecol. Modell.*, vol. 222, no. 1, pp. 33–47, 2011.

[145] W. J. Resetarits, "Colonization under threat of predation: avoidance of fish by an aquatic beetle, Tropisternus lateralis (Coleoptera: Hydrophilidae)," *Oecologia*, vol. 129, no. 1, pp. 155–160, 2001.

[146] M. Baldellou and S. P. Henzi, "Vigilance, predator detection and the presence of supernumerary males in vervet monkey troops," *Anim. Behav.*, vol. 43, no. 3, pp. 451–461, 1992.

[147] L. A. Isbell, "Predation on primates: ecological patterns and evolutionary consequences," *Evol. Anthropol. Issues, News, Rev.*, vol. 3, no. 2, pp. 61–71, 1994.

[148] R. J. F. Smith, "Alarm signals in fishes," *Rev. Fish Biol. Fish.*, vol. 2, no. 1, pp. 33–63, 1992.

[149] F. R. Walther, "Flight behaviour and avoidance of predators in Thomson's gazelle (Gazella thomsoni Guenther 1884)," *Behaviour*, vol. 34, no. 3, pp. 184–220, 1969.

[150] C. D. Fitzgibbon, "Anti-predator strategies of immature Thomson's gazelles: hiding and the prone response," *Anim. Behav.*, vol. 40, no. 5, pp. 846–855, 1990.

[151] C. D. Fitzgibbon, "Why do hunting cheetahs prefer male gazelles?," *Anim. Behav.*, vol. 40, no. 5, pp. 837–845, 1990.

[152] B. Heinrich, "Foraging strategies of caterpillars," *Oecologia*, vol. 42, no. 3, pp. 325–337, 1979.

[153] A. F. Hunter, "Gregariousness and repellent defences in the survival of phytophagous insects," *Oikos*, vol. 91, no. 2, pp. 213–224, 2000.

[154] A. Thornton and T. Clutton-Brock, "Social learning and the development of individual and group behaviour in mammal societies," *Philos. Trans. R. Soc. London.Series B, Biol. Sci.*, vol. 366, no. 1567, pp. 978–987, Apr. 2011.

[155] A. Le Roux, M. I. Cherry, L. Gygax, and M. B. Manser, "Vigilance behaviour and fitness consequences: comparing a solitary foraging and an obligate group-foraging mammal," *Behav. Ecol. Sociobiol.*, vol. 63, no. 8, pp. 1097–1107, 2009.

[156] I. K. Voellmy, I. B. Goncalves, M.-F. Barrette, S. L. Monfort, and M. B. Manser, "Mean fecal glucocorticoid metabolites are associated with vigilance, whereas immediate cortisol levels better reflect acute anti-predator responses in meerkats," *Horm. Behav.*, vol. 66, no. 5, pp. 759–765, 2014.

[157] N. Courbin *et al.*, "Reactive responses of zebras to lion encounters shape their predator-prey space game at large scale," *Oikos*, 2015.

[158] E. D. B. Jr, D. R. F. Jr, and E. D. B. III, "Predator avoidance and antipredator mechanisms:

distinct pathways to survival," *Ethol. Ecol. Evol.*, vol. 3, no. 1, pp. 73–77, 1991.

[159] X. Wang and X. Zou, "Modeling the Fear Effect in Predator–Prey Interactions with Adaptive Avoidance of Predators," *Bull. Math. Biol.*, vol. 79, no. 6, pp. 1325–1359, 2017.

[160] H. Matsuda, M. Hori, and P. A. Abrams, "Effects of predator-specific defence on biodiversity and community complexity in two-trophic-level communities," *Evol. Ecol.*, vol. 10, no. 1, pp. 13–28, 1996.

[161] P. Waltman, J. Braselton, and L. Braselton, "A mathematical model of a biological arms race with a dangerous prey," *J. Theor. Biol.*, vol. 218, no. 1, pp. 55–70, 2002.

[162] M. Moothedan and C. Joseph, "Survey on SLA for PaaS Clouds," vol. 6, no. 1, pp. 57–61, 2016.

[163] E. Brynjolfsson, P. Hofmann, and J. Jordan, "Cloud computing and electricity," *Commun. ACM*, vol. 53, no. 5, p. 32, 2010.

[164] S. Allesina and M. Pascual, "Network structure, predator - Prey modules, and stability in large food webs," *Theor. Ecol.*, vol. 1, no. 1, pp. 55–64, 2008.

[165] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," Springer, 2010, pp. 417–429.

[166] M. Glier and D. McAdams, "Concepts in biomimetic design: methods and tools to incorporate into a biomimetic design course," *ASME 2011*, 2011.

[167] H. Cheong and L. H. Shu, "Using templates and mapping strategies to support analogical transfer in biomimetic design," *Des. Stud.*, vol. 34, no. 6, pp. 706–728, 2013.

[168] T. Sullivan and F. Regan, "Biomimetic design of novel antifouling materials for application to environmental sensing technologies," *J. Ocean Technol.*, vol. 6, no. 4, pp. 42–54, 2011.

[169] F. S. Frillici, L. Fiorineschi, and G. Cascini, "Linking TRIZ to conceptual design

engineering approaches," *Procedia Eng.*, vol. 131, pp. 1031–1040, 2015.

[170] I. M. Ilevbare, D. Probert, and R. Phaal, "A review of TRIZ, and its benefits and challenges in practice," *Technovation*, vol. 33, no. 2–3. pp. 30–37, 2013.

[171] H. Beckmanna, "Method for transferring the 40 inventive principles to information technology and software," in *Procedia Engineering*, 2015, vol. 131, pp. 993–1001.

[172] D. Russo and C. Spreafico, "TRIZ 40 Inventive principles classification through FBS ontology," *Procedia Eng.*, vol. 131, pp. 737–746, 2015.

[173] S. P. Gorman, R. G. Kulkarni, L. A. Schintler, and R. R. Stough, "A predator prey approach to the network structure of cyberspace," in *Proceedings of the winter international synposium on Information and communication technologies*, 2004, pp. 1–6.

[174] M. Kumar, B. K. Mishra, and T. C. Panda, "Predator-prey models on interaction between Computer worms, Trojan horse and antivirus software inside a computer system," *Int. J. Secur. its Appl.*, vol. 10, no. 1, pp. 173–190, 2016.

[175] T. T. Director *et al.*, "ON THE CUSP OF EVOLUTIONARY CHANGE," 2013.

[176] W. Mazurczyk and E. Rzeszutko, "Security--A Perpetual War: Lessons from Nature," *IT Prof.*, vol. 17, no. 1, pp. 16–22, 2015.

[177] J. K. S. Nagel, R. L. Nagel, R. B. Stone, and D. A. McAdams, "Function-based, biologically inspired concept generation," *Artif. Intell. Eng. Des. Anal. Manuf.*, vol. 24, no. 4, pp. 521–535, 2010.

[178] D. Talia, "Clouds meet agents: Toward intelligent cloud services," *IEEE Internet Computing*, vol. 16, no. 2. pp. 78–81, 2012.

[179] Daniel Faggella, "What is Machine Learning?," 2017. [Online]. Available: https://www.techemergence.com/what-is-machine-learning/. [Accessed: 30-Jun-2018].

[180] Biology and O. Dictionary, "Predator-prey relationship." [Online]. Available: https://www.biology-online.org/dictionary/Predator-prey_relationship. [Accessed: 30-Jun-2018].

Key Terminology & Definitions

Bio-inspired – Inspired by methods and mechanisms in biological systems. This is a short version for biologically inspired, a cross-domain field of study that aims to bring together cross-domain concepts, methods, techniques, etc. Common areas of study include evolution (genetic algorithm), ants and termites (emergent systems), life (artificial life and cellular automa), immune system (artificial immune system), etc.

Artificial Life – This bio-inspired domain pertains to study of systems that have relation to natural life. Also, commonly referred to as Alife, this domain encompasses experimentation; simulation and modelling, of natural life processes (e.g. adaptive behaviours) and its evolution. For instance, one would study in biological life in order to construct a system that behaves like a living organism.

Cybersecurity – Cyber Security as a continuum of technologies and innovations for ensuring and assuring the security of data and networking technologies. the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data assets used in cyberspace. The concept includes guidelines, policies and collection of safeguards, technologies, tools and training to provide best protection for state of cyber environment and its users.

Cyberdefense – This refers to mechanisms (tools, techniques and strategies) implemented to defend cyberspace, especially critical infrastructure, against malicious and potentially catastrophic attacks. Proactive cyberdefense includes implied mechanisms implemented in anticipation of an attack. Aggressive cyberdefense is a form of proactive defense whereupon ethical hack back aims

to fight back attackers with an aim to frustrate and increase cost of attacks, track source of attack, or even destroy attack capabilities.

Survivability – Survivability has traditionally been described as a mission; i.e. a capability of a system to provide services in a timely manner bearing in mind that precautionary countermeasures will fail. Dependability, which is a property for a computing system to relied upon for delivery of a service placed upon it

Machine Learning – "Machine Learning is the science of getting computers to learn and act like humans do and improve their learning over time in autonomous fashion, by feeding them data and information in the form of observations and real-world interactions. It is part of research on artificial intelligence, seeking to provide knowledge to computers through data, observations and interacting with the world. That acquired knowledge allows computers to correctly generalize to new settings" [179].

Predator-Prey – "An interaction between two organisms of unlike species in which one of them acts as predator that captures and feeds on the other organism that serves as the prey. In ecology, predation is a mechanism of population control. Thus, when the number of predators is scarce the number of preys should rise. When this happens, the predators would be able to reproduce more and possibly change their hunting habits. As the number of predators rises, the number of prey decline"[180].

Mr. S N Mthunzi: *S N Mthunzi* is Doctoral student at Staffordshire University, Stoke-on-Trent, United Kingdom with research interest which includes Bio-inspired systems, Cloud computing and Cyber security and Survivability. His scholarly work also includes Digital Forensics, Computer Security and Ethical Hacking. Siyakha has published research papers in prestigious conferences including IEEE. He has previously worked in a Research and Development project

for Software testing as a Service. Siyakha is also a PTL in the School of Computing and Digital Technology at Staffordshire University. He is a member of the Cloud Computing and Applications Research Lab and Cybersecurity Research Lab, IEEE, and is a Fellow of Higher Education Academy (HEA). Siyakha is also a reviewer for Journals and International conferences.

e-mail: siyakha.mthunzi@research.staffs.ac.uk.

Affiliation/Address: Cloud Computing and Applications Research Lab, School of Computing and Digital Technologies, Staffordshire University, Mellor Building, College Road. Stoke-on-Trent, ST4 2DE

***Prof E Benkhelifa**:* is a Professor of Computer Science at Staffordshire University, UK, with an extensive experience in working with industry on real world business problems. Elhadj was (2014-2016) the Faculty Director of the Mobile Fusion Applied Research Centre (45 PhD students and 15+ Staff). Over the past years, Elhadj has built a rich portfolio of successful collaborative cutting edge research projects. Elhadj is the Founding Head of the Cloud Computing and Applications Research Lab and the Cybersecurity Research Lab, leading a team of 8 PhD Students and Research Staff. Elhadj has a strong research publications and dissemination track record and a co-founding chair of several pioneering conferences/workshops. Elhadj research very contemporary to cover many aspects of Cloud Computing including security, Mobile Cloud, Software Defined Systems, Cloud Forensics, IOT and Cloud, Fog and Mobile Edge Computing, Cloud computing resilience, Social Network Analysis, Collaborative software development, security as a service, testing as a service to mention but the most recent work. He has served as a guest Editor of many journals Special Issues, IEEE Trans Cloud Computing, Cluster Computing, Future Generation Computer System etc., and chaired several international conferences and workshops (IEEE FMEC 2017,

IEEE SDS 2017, IEEE IOTSMS 2017, IEEE MCSMS 2017, IEEE AICCSA 2016, IEEE GlobeCom-CCSNA 2017, IEEE ICICS 2017 and others). Elhadj delivered several keynote lectures at different prestigious venues. He is a Senior R&D Advisor to several companies in the UK and a member of several panels and committees within the UK and internationally.

e-mail: E.Benkhelifa@staffs.ac.uk.

Affiliation/Address: Cloud Computing and Applications Research Lab, School of Computing and Digital Technologies, Staffordshire University, Mellor Building, College Road. Stoke-on-Trent, ST4 2DE

***Dr T Bosakowski**:* is currently a lecturer in Computer Networks and Security at Staffordshire University. Previously, Dr Bosakowski has been a lecturer at Huddersfield University and an associate tutor at Edge Hill University. I am a member of the university's Cisco teaching team and a qualified CISCO CCNA and CCNA Security instructor. British Computer Society (BCS) , Associate Member of the BCS (AMBCS), 2011.

***Prof S Salim Hariri**:* is a Professor in the Department of Electrical and Computer Engineering at The University of Arizona. He received his Ph.D. in computer engineering from University of Southern California in 1986, and an MSc from The Ohio State University in 1982. He is the UA site director of NSF Center for Cloud and Autonomic Computing and he is the Editor-In-Chief for the CLUSTER COMPUTING JOURNAL (Springer, http://clus.edmgr.com) that presents research techniques and results in high speed networks, parallel and distributed computing, software tools, and network-centric applications. He is the Founder of the IEEE/ACM International Symposium on High Performance Distributed Computing (HPDC) and the co-founder of the IEEE/ACM International Conference on Autonomic Computing and ACM Cloud and Autonomic Computing

Conference. He is co-author/editor of four books on Autonomic computing, parallel and distributed computing: Autonomic Computing: Concepts, Infrastructure, and Applications (CRC Press, 2007), Tools and Environments for Parallel and Distributed Computing (Wiley, 2004), Virtual Computing: Concept, Design and Evaluation (Kluwer, 2001), and Active Middleware Services (Kluwer, 2000). Dr. Hariri developed innovative cybersecurity behavior analysis tools, resilient cloud services, and autonomic software tools.