Volume No:2, Issue No:2 (July-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Environmental and Cyber Security System

Dr.Ramana (Naik) Banothu
Professor & Principal,
Department of Computer Science and Engineering,
Trinity College of Engineering & Technology,
Peddapalli.

Dr.A.Arun Kumar
Professor,
Department of Computer Science and Engineering,
Balaji Institute of Technology & Science.
Narsampet.

ABSTRACT:

Current system security frameworks are dynamically demonstrating their restrictions. One trustworthy gauge is that lone around 45% of new dangers are distinguished. Thusly it is fundamental to locate another bearing that cyber security advancement ought to take after. We contend that the up and coming era of cyber security frameworks ought to look for motivation in nature. This approach has been utilized before as a part of the original of cyber security frameworks; be that as it may, from that point forward digital dangers and environment have developed fundamentally, and in like manner the original frameworks have lost their viability. An up and coming era of bio-motivated cyber security research is rising; however advance is obstructed by the absence of a structure for mapping organic security frameworks to their digital analogies. In this paper, utilizing phrasing and ideas from science, we depict a cyber security nature and a structure that might be utilized to methodically inquire about and create bio-enlivened cyber security.

Keywords:

Bio-inspired cyber security, cyber security ecology, bio-mimetic systems, cyber-ecosystem.

INTRODUCTION:

It's estimated that current commercially on hand anti-virus products are in a position to realize best forty five% of the brand new threats that internet customers face on a daily basis [1]. Additionally, the number and performance of malicious software utilized by way of cybercriminals, as well as its sophistication and complexity, is continually increasing. Hence, the usual size of time between initial injection of a hazard into the network and its discovery is growing every yr, and is now measured in months (in keeping with Verizon’s “2014 knowledge Breach Investigations report”), if now not years. Additionally, present safeguard systems are largely static and now not sufficiently adaptable to manage with the attackers’ changing tools and systems. The inability to furnish relied on secure offerings in modern-day verbal exchange networks might possibly have a giant socio-fiscal impact on both E2E and E2C global markets. Because presently on hand cyber defenses are regularly showing their obstacles, it's relevant to find a new course for cyber security study and progress to comply with. We endorse that the network protection neighborhood will have to look into nature for brand spanking new tactics to cyber security, both offensive and protecting.

Present and future cyber security solutions must be designed, developed, and deployed in a technique with the intention to completely leverage the expertise, learning, and abilities from on-going biological evolution. Conversely, the community must additionally look to nature to assume how the chance could evolve, and respond for that reason. Probably the most super pros and cons of the bio-encouraged cyber security procedure are distinctive beneath. First, nature has over 3.8 billion years of experience in setting up solutions and adaptations to the challenges that organisms face living in extremely numerous environmental conditions. The estimated number of (generally undiscovered) species is tens of hundreds of thousands, and each and every of them possesses distinct and distinctive characteristics facilitating survival and propagation of their own genes. The key method of dwelling organisms that has ended in the persistence of essentially the most effective types and behaviors is evolution. Evolution has developed gold standard options for instances analogous to the threats confronted by means of computer network programs. Second, for a long time individuals have sought inspiration from nature. Some principal present day examples include biomimicry, which is the thought of such innovations as Velcro tape and "cat's eyes" (retro reflective street markings). Computer science has additionally taken a page out of nature’s ebook with the aid of setting up biologically stimulated procedures like genetic algorithms, neural and sensor networks, and so on. Despite the fact that at first look there may not appear to be an instantaneous relationship between cyber security and the patterns reward in nature, closer inspection displays that the essence of most identified internet assaults and defense mechanisms has analogies in nature.

For example the Kudzu vine is capable to penetrate its ecosystem with an remarkable pace of ca. 30cm/day. Within a short time it can choke all different vegetation, together with trees and shrubs, with the aid of blockading entry to the resources necessary for survival – mild and vitamins and minerals. The essence is just like in DDoS (disbursed Denial of provider) assaults for communique networks where legit customers are deprived of the resources that they're entitled to love access to the carrier, bandwidth, CPU time, etc. Equivalent analogies can also be drawn for other offensive approaches as good as for safety solutions, as observed and described in [2]. One more strong analogy is the “palms race” (a form of a coevolution involving an aggressor constructing its offensive mechanisms and a sufferer/host evolving countermeasures in the type of protecting barriers). “arms race” is more often than not located between e.G. Predators and prey in nature. An identical dynamics may also be additionally found in interactions involving hosts and parasites, with the previous continuously seeking to invade host bodies and the latter consistently evolving countermeasures preventing the invasion. Each the abovementioned circumstances undergo many resemblances with a “malware-security methods” state of affairs (or extra probably “attackers-defenders”) the place there's a continual competition to enhance offensive/protective measures as fast as feasible to as a minimum briefly dominate the opposite facet. Thus, it's with no trouble obvious that in each nature and cyber world, entities have to evolve permanently and adapt to ever-altering Environments. In biology this phenomenon – an organism’s must consistently adapt and evolve to prevent extinction – is known as the pink Queen speculation [19]. It was once named after a character from Lewis Carroll’s book "by means of the looking-Glass". In this e-book the purple Queen described her country as a location where “…it takes the entire strolling you can do, to hold within the same place”. Precisely the identical method can also be located in cyber security and in organic systems the place there is a consistent want for adaptation of offensive/shielding approaches to maintain a targeted stage of adaptation allowing survival and replica/propagation.

Bio-influenced cyber security will not be a new thought. The primary generations of cyber security research were bio-prompted, e.G., the immune method stimulated protection approaches centered on signature evaluation, as well as ways for dealing with polymorphic threats (which can be analogous to, e.G., exceptional influenza lines). Considering the fact that then, nonetheless, the threats have evolved to make these first-generation defenses less mighty. So as to survive, cyber security have got to be developed/tailored for this reason to counter the brand new threats. A next generation of bio-encouraged cyber security study is now emerging; nonetheless, we find the expertise and achievements to be scattered because the field lacks a framework. This paper aims at filling this hole by way of defining, situated on the terminology and standards known from biology, the cyber security ecology (and related phrases). This cyber security ecology will permit a rigorous analysis of the existing relationships between entities in the cyber security ecosystem. Such a systematic view of cyber security will allow the study group to investigate and examine organic organisms' interactions with these from the virtual world with a purpose to identify variations, deficits and potentially new promising procedures to cyber security. We have got to be cautious, nevertheless, that the mappings from nature to the cyber world are usually not consistently "1-to-1", i.E., the analogies usually are not at all times superb. One of the crucial reasons that specified mappings are not normally possible include:

- Many mechanisms and relationships in nature are very intricate and no longer yet understood sufficiently to safely map them to the digital world;
- In nature, character organisms inside a species are disposable, and loss of life is a significant driver of evolutionary adaptation; but for a lot of protection-central techniques (e.G. Army, utilities, and different critical infrastructure) any loss, compromise, or corruption is unacceptable;
- The most important purpose for any organism is to outlive and reproduce, whereas our computers / networks have many exceptional targets (specific tasks and services).

Regardless of these imperfect mappings we strongly feel that there are nonetheless many major lessons from nature that can improvement and reinforce cyber security. Moreover, if we comply with a Sapir-Whorf hypothesis [31], which states that language has an immediate influence on ideas, and then finding analogies between cyber security and nature with its accompanying terminology, concepts and solutions can have a gigantic have an impact on the way in which we suppose about solving cyber security problems. New mechanisms and strategies may just emerge. Hence, the systematic view for bio-encouraged cyber security that we're proposing should aid to unveil new promising instructions that might be pursued to discover and improve strong subsequent-iteration security solutions. The relaxation of this paper is structured as follows. Section 2 summarizes the today's in bio-inspired cyber security. In part 3 the analogy between the biology-established ecosystem and the cyber-ecosystem, including knowledge interactions, is drawn. Section 4 describes some promising research instructions for cyber security. Ultimately, the final part concludes our work.

RELATED WORK:

The prevailing literature includes many makes an attempt to map biological principles to cyber security. And, many of these attempts have effectively transitioned to cyber security applied sciences and methods in common use this present day, together with anti-virus, intrusion detection, risk conduct evaluation, honey pots, counterattack, etc. [2]. As already recounted within the earlier part, present study on bio-inspired cyber security is fragmented and lacks a scientific approach. A primary rationale is the variety of features from nature that can be used as notion for cyber security study. Current study is also extensively segmented into two corporations, depending on how an idea is drawn:

•When thought is drawn from a given organism's characteristic feature/security mechanism (internal or outside). Interior mechanisms comprise, for illustration, an immune method. Outside mechanisms incorporate e. G. Quite a lot of camouflage and mimicry tactics;

•When proposal is drawn from various inter-organism interactions – this entails,e. G., predator-prey associations.

2.1 Bio-influenced cyber security prompted with the aid of an organism's attribute function/safety mechanism:

with a view to readily preclude detection/remark an organism can conceal or conceal its presence with the aid of utilizing camouflage or mimicry techniques that adjust the organism's outside appearance [17]. Camouflage embraces all solutions that make use of person's physical shape, texture, coloration, illumination, and many others. To make animals tricky to spot. This motives the know-how about their detailed region to stay ambiguous. Examples of animals that may comfortably combination into the background incorporate the chameleon (household Chameleonidae) which is able to shift its skin color to make it much like ambient lighting and history coloration; stick and leaf bugs (order Phasmotodea) that take the bodily form of a wood stick or a leaf; orchid mantis (Hymenopuscoronatus) that resembles a tropical orchid which, even though rather conspicuous, is complicated to detect towards a history of developed vegetation. Camouflage in most cases happens on stages rather then visual realization: e.G., many viruses code pathways and molecular signaling methods that mimic host cellphone transduction mechanisms – by doing so the virus can with ease invade the mobile phone and take control of the metabolism and immunological system of an person [20].

In cyber space quite a lot of information hiding methods, e. G. Steganography, may also be utilized to provide manner to hide the location of personal information within an innocent-looking service or to otherwise allow covert conversation across communication networks [18]. Patterns and/or colorings can be also used to confuse the predator, i.E., to make knowledge in regards to the prey hard to interpret. Such so-known as "disruptive" camouflage is possible and can also be seen in, e.G., a herd of zebras (Equusquagga) the place it is complex for an attacking lion to identify a single animal in a herd once they flee in panic. Patterns of contrasting stripes purportedly degrade an observer's capability to guage the velocity and path of moving prey, they usually accomplish that through exploiting distinct mechanisms associated with the best way mind approaches visible expertise on action [21].

A similar thought is utilized by using quite a lot of moving goal tactics/safeguard in our on-line world, which distribute the uncertainty between the attacker and the defender extra rather. For illustration, some first-generation options made periodic changes in a number's appearance from the community perspective, in order to mitigate the effectiveness of target reconnaissance [8]. 2d-generation options comprise, e.G., an ant-headquartered cyber safety which is a mobile resilient security procedure that eliminates attackers' capacity to rely on prior expertise, with out requiring movement in the included infrastructure [12].

Mimicry characterizes the instances wherein an organism's attributes are obfuscated via adopting the traits of another residing organism. In distinct, because of this the prey can preclude attack by means of making the predator feel it's some thing else, e.G., a innocent species can mimic a unsafe one. The prey hides expertise about its own identification by using impersonating something that it is not. For example, harmless milk snakes (Lampropeltis sp.) mimic venomous coral snakes (Micrurus sp.) to confuse predators that are less prone to launch an assault in expectation of a venomous harmful bite. Cybersecurity solutions that utilize the identical inspiration comprise various site visitors style obfuscation techniques, e.G., site visitors morphing [16].

Organisms' internal techniques may also encourage new cyber security strategies. There are many contemporary experiences trying to map features and capabilities of the human immune method to cyber area [3, 9, 10, 11]. Immune programs use a range of receptors to become aware of external antigens (alien proteins). These variants are usually not inherited but alternatively are generated via recombination within the procedure of V(D)J (somatic) recombination, which generates repertoires of receptors present process clonal decision and reinforcement – preparing them for amazing motion towards antigens, with the bottom feasible level of autoagression (e.G. Reaction against an organism's own proteins) [22]. The consequent synthetic Immune methods (AIS) are designed to imitate unique houses of the usual immune approach. In cyber security their principal application is anomaly and misbehavior detection. AIS more commonly depend on one in every of 4 main paradigms: (i) poor determination algorithm [3]; (ii) clonal resolution algorithm [9]; (iii) dendritic cell algorithm [10] or (iv) idiotypic networks models algorithms [11]. The first generation AIS (i and ii) utilized most effective simple items of human immune techniques, so the resulting efficiency was not comparable with its human counterpart. Latest AIS (iii and iv) are extra rigorous and higher correspond to average immune programs.

2.2 Bio-prompted cyber security stimulated by using organisms' interactions in nature, there are numerous interactions between organisms that possibly could serve as inspirations for cyber security.

For illustration, several reviews center of attention on more than a few elements of predator-prey associations. In [13] the authors make the predator-prey analogy for the web and investigate how exclusive stages of species diversification can serve as a defensive measure. They viewed each and every style of a inclined gadget as a heterogeneous species and investigated what degree of species diversification is critical to restrict a malicious assault from causing a failure to the whole community. Subsequently, in [5] it was once learned that the rate to the predator in searching for its prey enormously affects the predation system. In specific it has been observed that even particularly simple approaches for elevating the fee of predation can effect in colossal reduction in outbreak measurement. Different reports utilize organic items of epidemic spreading (a targeted case of adverse interaction between the pathogen and the sufferer) to predict or analyze malware outbreaks [14], [15].

Ultimately, the relationships and interactions between current malware (so called malware ecology) were investigated in [6]. Numbers of interactions, each unintentional and intentional, between extraordinary forms of malware had been analyzed and the principal conclusion used to be to seek ecologically-inspired safety techniques, on account that many strategies from ecology can also be immediately utilized to all points of malware protection. From the experiences awarded above we are able to conclude that bio-stimulated cyber security is a large, various, emerging, and evolving research field. However, from the research standpoint, we see many "unfastened ends" that need to be tied by way of utilizing a extra systematic method, which we subsequent recommend.

3. CYBERSECURITY ECOLOGY:

In this section, first we systematically evaluation the key phrases from biology regarding ecology. Then by way of borrowing and adjusting the usual biology-established definitions, we will describe the important add-ons of cyber-ecosystem and then of cybersecurity ecology.

3.1 Cyber-ecosystem:

In biology the term ecology is outlined as the area of existence sciences inspecting and finding out interactions amongst organisms and/or their environment. Because of this it deals with the structure and functioning of ecosystems. An ecosystem is outlined as a neighborhood of residing organisms (biotic components) in conjunction with the nonliving (abiotic) components of their atmosphere that engage as a procedure. Apart from the biotic and abiotic accessories, interconnected by means of quite a lot of interactions, the ecosystem is fueled by way of energy, quite often in the form of electromagnetic radiation (if production in an ecosystem is sun-pushed, i.E. Accomplished with the aid of inexperienced crops) and chemical vigour (if an ecosystem relies on chemosynthetic micro organism). Both biotic and abiotic causes can influence an organism.

For illustration, climate trade or an atypically enormous quantity of predators can negatively have an impact on some species [23]. In each ecosystem the power waft is relevant as each ecosystem is power-centered and is ready of remodeling, gathering, and circulating vigour. In nature the flow of energy is encapsulated in a food chain, and a notion of trophic phases is utilized to illustrate the role that an organism occupies in a food chain (Fig. 1, left). Relying on how vigor is acquired, two companies of organisms will also be extraordinary: producers (which are able to fabricate their possess meals utilizing inorganic components and chemical/radiation power) and consumers (that feed on producers and/or other patrons) [24].

Ecology can be seen as one of the techniques to study intricate and dynamic techniques. For that reason, if we're able to recognize how ecosystems and related concepts map to the cybersecurity area then the usefulness of quite a lot of ecological methodologies will also be evaluated. If such mappings are successful then application of many mathematical ecological techniques models to cyber techniques will also be investigated. Based on the above phrases and definitions from ecology, we wish to systematically recreate a similar taxonomy for the cyber world. Let us define cyber-ecosystem as a neighborhood of cyber-organisms i.E. Non-human actors e.G.

Applications, processes, packages, protecting and offensive systems (analogues to the biotic components) that have interaction between themselves and with the atmosphere (abiotic accessories). Allow us to additionally anticipate that the atmosphere in which biotic components live and interact is a communiqué network, e.G. The web, and it constitutes a nonliving (abiotic) element with its hardware, hyperlinks and interconnections. In the cyber-ecosystem (the same as in nature) each biotic and abiotic reasons can have an impact on a cyber-organism. For example, malicious software will also be utilized to compromise a user's device defenses and steal his/her confidential information. On the other hand a failure of the hyperlink/networking device or network congestion have an effect on a cyber-organism's capability to be in contact and exchange understanding. In one of these outlined cyber-ecosystem we're certainly interested in the network of interactions amongst cyber-organisms, and between cyber-organisms and their environment. As recounted above, in nature the key resource is vigour. In communication networks, the analogous key resource is special forms of knowledge, including person private or person-generated data, but in addition information about his/her conduct. In this kind of cyber-ecosystem, expertise may also be transformed, collected, and/or circulated (much like vigour in ecosystems). To have more clear analogies between ecosystems and cyber-ecosystems the function of the humans in the gift context is restrained to these roles:

- Producers which possess and generate knowledge that forms a fascinating useful resource for the customers (e.G. The tools that attackers or digital advertising and marketing companies use to receive preferred knowledge).
- Accessories of the offensive/protective solutions. For instance, a bot herder in general issues command to the bot that he controls so he's an inevitable “phase” of the botnet. One other example is an identification/PS (Intrusion Detection/Prevention approach) which is configured and monitored through a protection professional.
- A part of “evolutionary force”. People have an impact on cyber-organisms by altering their code, functionalities and applications. In this approach an evolution is achieved. Quite often, attackers attempt to outwit the defenders through setting up malicious application so as to be ready of overcoming existing defense mechanisms / methods. Conversely, defenders boost their defenses to be “immune” to the

existing threats. As a result, both sides are collaborating in a cyber “palms race”. Due to the fact that the above, it's possible also for the cyber world to characterize distinct “cyber meals chains” and/or cyber-trophic levels (Fig. 1, correct). Consumers can turn out to be cyber-predator (attacker) or cyber-prey (defender) relying on the location in the cyber food chain. Producers always take the function of cyber-prey.

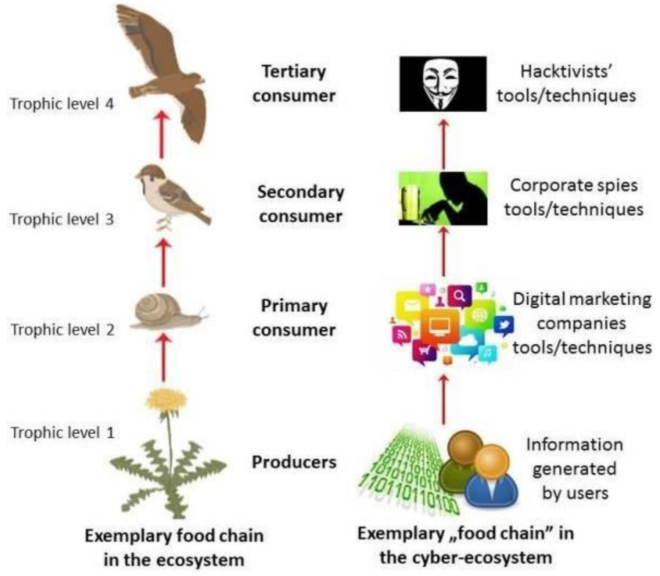

Trophic level 4
Tertiary consumer
Hacktivists' tools/techniques
Trophic level 3
Secondary consumer
Corporate spies tools/techniques
Trophic level 2
Primary consumer
Digital marketing companies tools/techniques
Trophic level 1
Producers
Information generated by users
Exemplary food chain in the ecosystem
Exemplary „food chain" in the cyber-ecosystem

Fig. 1 Food chains and trophic levels in an exemplary ecosystem (left) and a cyber-ecosystem (right).

By the use of a easy analogy we can outline the next terms that carefully describe the toolbox of cyber security ecology: Cyber Ecology (CE) as a area that analyzes and stories interaction amongst cyber-organisms and/or their environment. Cyber security Ecology (CSE) analyzes and reviews interactions amongst cyber-organisms and between cyber-organisms and their atmosphere that impact their protection. CSE is a subfield of CE. Attacker–Defender Ecology (ADE) describes interactions between cyber-organisms which take roles of attackers and defenders within the detailed cyber-ecosystem (e. G. In the internet).As famous before such relationship may also be viewed no longer handiest as predation but in addition as parasitism. It's also valued at noting that such interactions dwell in extraordinary places of the cyber food chain and depend on the trophic degree (Fig. 1). ADE is a part of CSE. Attackers Ecology (AE) illustrates interactions between attackers (cyber-organisms) in a given cyber-ecosystem. The possible interactions embody each opposed and non-hostile ones and rely upon the context. Attackers can predate or parasite on every other, however the relationship may also be of a symbiotic or a cooperative nature. AE is a part of CSE. Defenders Ecology (DE) presents insights into abilities interactions between the defenders (cyber-organisms), and it contains generally non-adversarial ones. It includes both outside defense mechanisms (interactions of malware and protection systems resulting in defense) and inner residences (analogous to animal immune systems). DE is a part of CSE.

The above mentioned terms e. G. AE may also be further divided into e. G. Malware ecology, botnet ecology, and many others. The relationships between the terms defined in this and in prior sections are illustrated in Fig. 2.

3.3 Cyber-Ecosystem Interactions:

The structure and stability of an ecosystem in nature will depend on the set of interactions that interconnect different entities. Interactions may also be roughly categorised into antagonistic interactions (between species; regularly predation and parasitism), non-hostile interactions (between and inside species; cooperation, symbiosis)

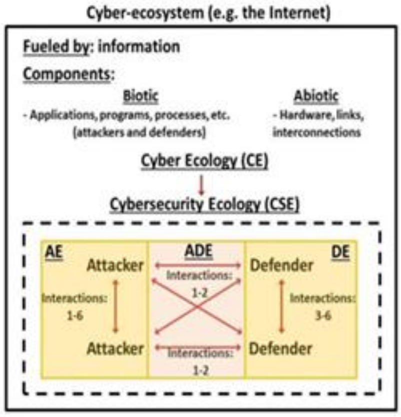


Fig. 2 Main components and interactions in a cyber-ecosystem (Interactions: 1-predation, 2-parasitism, 3-symbiosis, 4-cooperation, 5-sexual interactions, 6-competition).

And sexual resolution-driven interactions (within species). In all three lessons, interacting entities coevolve, responding reciprocally to their current states in a confident/negative suggestions loop mechanism (also known as the palms-race dynamics for hostile interactions) [23]. The interactions will also be outlined as follows:

- predation: a technique of acquiring resources by way of killing/eating our bodies of different organisms; results in the demise of the prey; predation involves difficult cycles of prey and predator abundances described with the aid of mathematical items such because the Lotka-Volterra equations procedure ([23], [25]), which may also be utilized to design probably the most gold standard tactics of protection or offense, relying on which side of the predation-prey system the focal cyber-organism currently is. In communique networks ransomware can also be dealt with as a predator as it is "killing" the host through encrypting imperative know-how it retailers and until the ransom is paid this useful resource is "destroyed/lost" i.E. Consumer's information cannot be retrieved;
- parasitism: interplay involving obtaining assets through consuming other entities however now not killing them [23], [25]; it gave upward thrust to a fruitful area of epidemiological parasitology, with mathematical units and defense methods that would be instantly implemented in the context of cyber-epidemics. As already mentioned the current pattern, above all for sophisticated malware corresponding to evolved chronic Threats (APTs), is more much like a parasite-host scenario than a predation-prey one. It implies that it's extra probably that the malicious application might be lively on an contaminated host for a very long time and obtaining its assets in a obvious method; symbiosis: positive interaction involving obligatory interplay of two or extra entities, crucial for all parties for survival and positive propagation. In cybersecurity this could incorporate analysis of each attackers and defenders symbiosis. For example, for malware contamination situation it is customary that the primary infection is in the beginning carried out by means of exploiting some vulnerability on the host computing device and this allows later for the 2d a part of malware to be downloaded and achieved to be able to participate in malicious actions for the cybercriminal;
- cooperation: facultative interaction of an character within one species or individuals of distinct species, increasing the health and survival of different contributors (the acceptors of cooperation) probably on the cost of the focal man or woman (the giver of cooperative behavior) [23], [26], [27]; in conversation networks cooperation will have to be well-known now not most effective as a way of reinforcing protection mechanisms but additionally as a abilities risk (a deceiver malware would make the most cooperating inclination of the method, wreaking havoc in its buildings). A recent real-world example is the sharing of cyber chance symptoms as prescribed in the united states Cyber security understanding Sharing Act of 2015;
- sexual interactions: occur solely inside species and are channeled towards combining, in probably the most desired and robust manner, the genes of girls and men in order that they maximize the fitness of offspring [28]; from the factor of view of cyber-ecosystems the items of sexual choice established on compatible genes [29] are principally fascinating as they will function mechanisms for based on compatible genes [29] are particularly interesting as they may serve as mechanisms for producing dynamic sets of the most optimal combinations of entities and their mutations that provide maximum protection against evolving malware. Moreover, using knowledge of how sexual selection works, it may be interesting to study how to become the most

"unattractive" victim to the potential attacker.

- competition: this relationship is symmetrical and involves both organisms competing for the same pool of resources. Inherently the relationship between organisms can be broken without any harm to neither of the sides – as both influences are negative their cessation benefits both competitors. In communication network environment this interaction can occur e.g. between two types of malware trying to infect the same host – when one of them succeeds it tries to "secure" the host by patching the exploit used by the other type of malicious software. Competition can also occur between defenders when few similar defense systems (e.g. anti-virus software) are run together and they impact each other in a negative way.

A point of view of cyber-ecology may be to treat these interactions as purely mechanistic descriptions of cyber-systems – without looking at the consequences of interactions themselves and on the dynamics they describe. However, growing evidence suggests that the interactions not only influence the fitness and performance of entities but also significantly modify their physiology /performance in the interaction, altering the outcome of competition/synergy [30]. Such elastic responses of interacting entities to the interaction itself may have a significant role in cyber-ecosystems, as they may serve to design more efficient ways of controlling cyber-ecosystems and reacting to unknown, emerging threats. As indicated in Section II, existing work focuses mainly on predator-prey association. However, an interesting observation is that the relationship between current malware and host is in essence closer to parasitism than to predation. This means that the goal of the current malware is to live off the infected host (and the longer it remains undetected, the better) but not to immediately cause significant harm or permanent damage.

In The subject of adverse interactions in ecological studies has sofar been dominated by a very sharp big difference between predator-prey interactions and parasite-host interactions. As mentioned lately such interactions are, nonetheless,a lot toward each other, and along side a 3rd category (competition) type a unified team of adversarial interactions involving the aggressor, the victim andassets that are/may just be to be had toone or each ecology", and encompasses all interactions involving unsafe effects of one organism on yet another, be it an immediate or oblique (e.G. Through shared resources) outcome. On this part we discuss penalties of this kind of categorization and review probably the most distinguished items of hostile interactions, whilst pinpointing their weaknesses [32].

4.1. Similarities between parasitic and predatory interactions the robust distinction between parasitic and predatory relationships outcome probably from an old methodology of categorizing nature [33]. Correctly, all sorts of hostile ecological interactions (predation, parasitism and competition) share a original suite of accessories, which differ best within the strength/presence/dimect personality of the exact connections. All interactions involve conventionally at the least two organisms (aggressor and victim, or two competitors in the competitors model) that impact each and every other positively and/or negatively, and use each and every others' assets [32]. -competitors: the least opposed of all interactions; the roles of the interacting organisms are indistinguishable and each exert together negative influence on the opposite.

The relationship is symmetrical and includes both organisms competing for the identical pool of resources. Inherently the connection between organisms can be broken without any damage finished to neither of the edges: as both influences are poor their cessation advantages each opponents [32].

Predation: happens when the aggressor kills the sufferer directly and feeds on its tissue – for this reason it is inherently asymmetrical; predation involves very quick time-scales, a lot shorter than timescales imperative for the evolution of low-degree (molecular, immunological) security mechanisms and, as a consequence, prey evolves defenses in such procedure more often than not at the bigger, organismal (e.G.Morphology and habits) stage [34]. Alternatively of immunological mechanisms prey advantages more by way of evolving learning-like mechanisms which are much more flexible on one hand and can evolve inside lengthy new release occasions on the other hand. On the grounds that predators consume their victims, they are considered as living on a different, better trophic stage than prey [32].

Competition: the least opposed of all interactions; the roles of the interacting organisms are indistinguishable and each exert together poor impact on the other. The relationship is symmetrical and involves both organisms competing for the same pool of resources. Inherently the connection between organisms can be damaged without any damage achieved to neither of the sides: as both influences are poor their cessation benefits both opponents [32].

Predation: happens when the aggressor kills the sufferer directly and feeds on its tissue – therefore it is inherently asymmetrical; predation entails very short time-scales, much shorter than timescales critical for the evolution of low-stage (molecular, immunological) safeguard mechanisms and, as a consequence, prey evolves defenses in such procedure normally at the higher, organismal (e.G.Morphology and conduct) level [34]. As a substitute of immunological mechanisms prey advantages extra via evolving studying-like mechanisms which are much more flexible on one hand and can evolve inside lengthy new release times on the other hand. Considering the fact that predators devour their victims, they are regarded as living on one more, bigger trophic stage than prey [32]. Parasitism: on this type of interaction the aggressor feeds on the sufferer however does not kill it. Predatory interactions are inherently deadly whereas parasitic interactions have resulted in the phenomenon of intermediate virulence, which maximizes parasite transmission to different hosts. The relationship between parasites and hosts is so much more intimate and occurs at time-scales and new release instances that enable the evolution of difficult genetic (e.G. Bacterial Crispr-Cas [35])and immunological (e.G.Vertebrate acquired immunity, invertebrate Toll receptors) safeguard mechanisms in victims/hosts. It is clear that all three ion ships are fairly unique and contain different phases of inter-organismal contact.

Nevertheless all of them draw from the same populace approaches Involving populace development and decline. Additionally, often parasitism and predation are tough to delineate. For instance, caterpillars feeding on plants would be viewed as predators, but they do not kill their victims and dwell on the surface of victim, as ectoparasites. Mosquitos feed on the tissues of their victims (like parasites) but aside from this they show many residences of predators (longer iteration time, quick interplay timescale, high turnover rate of attacked victims). Up to date literature has also mentioned that although seemingly different, parasitic and predatory interactions may give rise to identical ecological patterns. Some distinguished examples include:

- The evolution of inducible defenses and assault anticipation [36]: predation is most often associated with behaviors and qualities that are active and use resources best in the presence of predators – an identical mechanisms is also reward within the parasite-host techniques the place organismal systems (e.G. Immunological) may optimize their pastime window to match the pastime window of aggressors,

- Enemy-mediated facilitation [37]: within the presence of multiple aggressor, host/prey communities may evolve mechanisms that make use of prey-targeted resistance to aggressors and oblique ecological results that effect from version in prey/host susceptibility to aggressors,
- Managing the edge of transmission: in parasite-host programs there are unique host densities under which parasites are unable to effectively unfold and persist; a an identical suggestion probably applied to the predator-prey methods, where through managing the densities of certain predators ("superpredators" that impact prey densities essentially the most) the populace is also maintained at a favored degree of prey density, averting extinction as a result of random fluctuations in predation pressures [32]. Four.2. Items of hostile interactions

The ecological literature has developed a number of mathematical descriptions of the predator-prey or parasite-host interactions and no longer extraordinarily, and in keeping with the abovementioned unifying concerns, all these items can be adjusted for the outline of both predation and parasitism interactions. The most distinguished and the oldest mannequin is the Lotka-Volterra (L-V) model [33] that binds collectively aggressor and sufferer densities and models alterations in these densities according to an assumed predation/parasitism expense. The model is defined utilizing a procedure of two differential equations: = − ′ + ′ where x and y denote prey and predator densities, r and r' describe population progress/decline of prey/predator populations, whereas a/a' quantify the fee of encounters between prey and predators. The solution of this system describes the oscillatory habits of prey and predator densities. The L-V model was once rapidly regarded simplistic (e.G. The idea of constant encounter charges a/a' used to be regarded as biologically unrealistic) and a quantity of different models were developed. However, ecologists agree that every one available models are just certain circumstances of the L-V mannequin, which in turn nonetheless remains the fundamental model for adverse interactions amongst organisms [33]. The items that adopted the L-V procedure centered regularly on making a few of its assumptions extra practical. For example, the Nicholson-Bailey model multiplied on the outcome from the L-V procedure and generalized them to discrete generations of prey and predators (the L-V method used to be developed beneath the belief of continuous overlapping generations). Extra developed items, e.G. The Hollingmodel [38], the Ivlev model [39], and the Watt mannequin [40] remained within the fact set by using the Lotka-Volterra model, altering and adjusting most effective the come across perform (i.E.The operate that binds prey and predator densities at the side of time, offering the dynamics of the encounter premiums between interacting contributors). A right integration of the present units into the subject of cybersecurity will possible involve a revision of the assumptions of distinctive items of hostile interactions and relating them to the particular features of communication networks. Designated comparisons are imperative to clarify the shared features and assumptions at the interface of biological and cyber methods – such comparative analysis can then determine models which are the most accurate in describing cyber reality with respect to the hostile interactions.

4.3 hostile (parasitic) mimicry: Batesian mimicry Even without clear exploitation of fabric resources of the hosts, parasitism will also be reward if expertise content material/reliability is being exploited by one organism at the rate of the bills born by the opposite organism [41]. One good-documented instance of such behavior is parasitic mimicry, which is reasonably low-cost to the mimicking organism as it isn't associated with weapons/toxins this organism is pretending to have [42]. A recognized example is the Chrysotoxumfestivum hoverfly that resembles poisonous and stinging insects from the Hymenoptera staff. Through expressing warning colours the hoverfly avoids being attacked and eaten, and on the other hand it does now not have got to make investments assets in honestly having a sting. Parasitic (Batesian) mimicry, as a result of its low-cost nature, could quite simply be utilized in safety functions in cyber techniques. The mimic could be the security algorithm that might adopt some facets of the exact adverse software to procedure it and infiltrate without being detected [41]. Most existing items of Batesian mimicry function on the stability between charges of being detected and the advantages of expressing specific overlaying phenotypes. Such units would be used to derive parameter levels that make certain full overlaying in the cyber-ecosystem at the fee of the bottom feasible resource allocation.

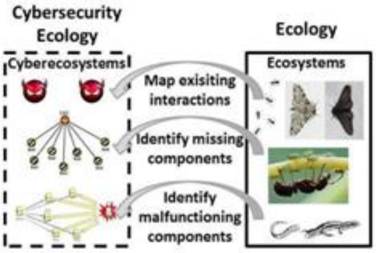
4.4 Non-opposed interactions Non-antagonistic interactions are more elaborate to classify and organize, on the whole seeing that they combine intra- and inter-species strategies. There exists no single mannequin of synergistic interactions similar to the seminal Lotka-Volterra mannequin; nevertheless, we've got a couple of methods of expressing the dynamics of such interactions mathematically. Non-adverse interactions that play important roles in development of cybersecurity solutions embody the entire above sexual selection/mate option processes, and symbiotic interactions. Both have the potential to greatly inform efforts to improve potent cybersecurity methods; both also stay largely unstudied on a colossal, inter-species comparative degree and therefore are attractive targets of comparative organic research.

4.5 Symbiotic interactions Symbiosis is concept to underlie all lifestyles in the world as, consistent with the end osymbios is hypothesis, all eukaryotic cells are descendants of a number of prokaryotic organisms that merged collectively as symbionts, which gave rise to currently located organelles such us chloroplasts and mitochondria [43]. Presently essentially the most in most cases known and good-studied examples of such interactions may just serve as excellent models to derive mathematical parameters that can be utilized in constructing cyber security solutions. From an evolutionary point of view, the symbiotic interactions will also be without problems modelled utilizing the equal mathematical reasoning as the one used in the Lotka-Volterra process, with the aid of modifying parameters of the equations so that interacting items improvement every different alternatively of harming [44].

From the point of view of cybersecurity applications, symbiotic interactions may potentially play roles in two scenarios. For one, symbionts in a cyber-ecosystem would be used to improve the protecting/immunizing effects of utilized procedures. Multiple symbiotic entities might put into effect every others' defensive procedures and attain fuller safeguard of the whole procedure. Alternatively, symbiotic interactions are intricately related to different close interactions. Actually, the Lotka-Volterra-like mannequin of symbiotic interactions [44] predicts that they can effortlessly turn into parasitic interactions if conditions shift in the environment of symbionts (e.G. If on hand assets grow to be extra asymmetrically exploited by using one of the most symbionts).

For this reason, such models are additionally in a position to furnish a checking out area where a variety of parameters that keep the necessary symbiotic interactions might be confirmed. Correctly, such units can also be used to derive replacement situations of combating cyber parasites – whether it is possible to "mutate" them and alter their responsiveness to the atmosphere – altering a parasitic interaction right into a symbiotic one with an artificially introduced extra organism [45]. A exact case of synergistic interactions occurs in cooperating organisms when contributors bear expenditures (as a rule the easiest fitness charges, i.E. Via suspending/totally leaving behind copy) and advantage other individuals by way of helping them (by and large within the form of raising their offspring) [27]. The dynamics of such interactions is first-class known in the altruistic forms of cooperation, where it is predicted and described through the Hamilton inequality [46] that binds expenditures of the donor, improvement of the receiver, and their coefficient of relatedness that defines how expenditures and advantages are balanced on both sides of the interaction [46], [47]. Within the context of this mission, however, it is of a marginal significance – rather more principal types of cooperating interactions will be these encountered between non-associated individuals. Such non-relations cooperation can comfortably be incorporated in our process (as reciprocal sharing of expenditures and executed advantages), nevertheless this discipline of ecology continues to be strongly underrepresented and no quantitative models exist that could be used and developed within the context of the proposed task.

4.6 Sexual choice From the point of view of cyber security, sexual determination may be the most elaborate but also the most effective interplay that could be exploited [48]. The most important drawback comes from the fact that sexual resolution operates via option of the most suitable mates and accordingly would require developing and keeping a populace of sexually reproducing entities that might use cycles of resolution in an effort to evolve new, extra potent ways of fighting enemy program [28]. It's an principal question how such decision would function and presently evolutionary biology describes two primary lessons of sexual resolution mechanisms. The primary one, referred to as "the great genes speculation" poses that selective members (in nature mostly women) choose special companions (on the whole adult males) in view that they furnish them with "just right genes" that broaden offspring viability and fitness [49]. Such indirect genetic advantages have been confirmed in many animal experiences and are a good-documented, even though nonetheless weakly understood phenomenon [28], [29]. The 2d category of sexual decision drivers falls into the "Fisherian runaway" class, where the choice of one sex (girls) evolves as a self-perpetuating mechanism that exploits targeted male traits and is fueled by using a constructive feedback loop generated by means of the powerful genetic correlations between feminine option and male display features [48], [49]. This 2d form of sexual decision has also been urged to occur in nature – however it's way more complicated to search out its location in the cybersecurity truth as this type of sexual choice is not straight related to any Fitness advantages to females (apart from picking adult males that can simply have the funds for to have exaggerated and overgrown qualities).


Cybersecurity Ecology
Ecology
Cyberecosystems
Ecosystems
Map exisiting interactions
Identify missing components
Identify malfunctioning components

Each items of sexual choice are governed with the aid of one usual mathematical model [50] that integrates feminine option (P), male display (D) and residual fitness effects (F). If we denote variance and covariance of distinctive traits as V and C (e.G. V(P) – variance in selection; C(PD) – covariance between display and preference), b_s and b_n as respective determination gradients due to sexual (s) and traditional (n) choice, the joint dynamics of these features is also described as:

```
_
          ( )     (  )        (  )        _ ( )

( ̅) = (   .         ( )      (    )) × ([ _  (  )] +
_
          .          .             ( )          _ ( )
                 _ ( )           ( )
            [ _ (  )]) + ( (  )),
                _ ( )           ( )
```

The place u denotes respective changes in phenotypes' values because of mutation. Distinctive combinations of parameters of this mannequin yield one-of-a-kind modes of sexual determination, and exploration of these values inside the degrees that are realistic to cyber methods will help uncover forms of interactions that may be the most effective in cyber security purposes After defining key words involving cyber security ecology, and describing fundamental items that signify interactions between organisms in nature, the next move is to strengthen a "process" in order to outcome within the talents new research recommendations. The steps of the sort of process involving interactions are illustrated in Fig. 3. Fig. 3 Comparing interactions and components between ecology and cyber security ecology.

First, it's most important to map existing offensive/protective measures as well as interactions in both varieties of ecosystems. From the biology viewpoint this involves performing rigorous meta-analyses describing comparatively and phylogenetically the variety of defense/offense mechanisms present in nature and their complexity (e.G. Their charges, probably the most optimum uses, their diversity at more than a few stage of lifestyles institution). In the next move, the lacking components within the digital world that might be possibly ported from nature will have to be identified. All of the most promising candidates that should not have counterparts in cyber area will type a record of most compatible bio-inspirations. Within the final step, it's also feasible to determine safety-associated add-ons that exist in cyber security however that aren't sufficiently robust. Then, insights from mechanisms and relationships that exist in nature could provide essential suggestions on how these protection tactics could be elevated.

To summarize, we think that currently probably the most promising research guidelines comprise:

- Drawing additional inspirations from the distinctive organism's characteristic function/safeguard mechanism. For example, such elements like aposematism (warning signal that's associated with the unprofitability of a prey object to talents predators) or autotomy (the place an animal sheds or discards one or more of its own physique parts to elude or distract the predator) might easily emerge as an proposal for future cybersecurity options.
- cautious investigation and applying abilities from the recounted nature-established interactions. As already observed the malware-host scenario is extra similar to parasite-host than to predator-prey association. Hence, more study concentration should be grew to become to the models and achievements of biology in this area. This might furnish many new, interesting insights. A different research path that we consider has not been sufficiently explored is sexual interactions where e.G. The approaches to become an appealing/unattractive target might be analyzed.
- Comparative evaluation of the elements of parasitic and predatory techniques that expose their usual underlying mechanisms leading to their description within the natural enemy framework. Such usual properties of those antagonistically interacting systems is also the most effective features (in a technique identified by long evolutionary historical past of such systems) where new procedures to cybersecurity can also be developed. on/anticipatory mechanisms that lessen the bills of preserving energetic safeguard mechanisms; (ii) enemy-driven Essentially the most promising avenues on this crew of problems comprise (i)

brought facilitation – which, by using exploiting more than one enemies, may result in the establishment of reinforcement mechanisms that develop the effectiveness of enemy elimination; (iii) transmission threshold management which is able to provide instruments to lower the trouble in disposing of threats, even as maximizing the performed safety acquire.

CONCLUSION:

This paper offers a systematic ecology-based procedure to cyber security. Based on the statement of the huge fragmentation of achievements and expertise within the discipline of bio-influenced cyber security, we propose a cyber-ecosystem, cyber security ecology, and associated terminology which may be used to be trained offensive/shielding mechanisms and interactions amongst cyber-organisms and/or between cyber-organisms and their environment. In our opinion this helps to determine new expertise future research guidelines for bio-motivated cyber security.

References:

[1]D. Yardon, “Symantec Develops New Attack on Cyber hacking”, Wall Street Journal, May 2014, URL: http://www.wsj.com/articles/SB100014240527023034171045795421 40235850578

[2]W. Mazurczyk, E. Rzeszutko, Security – a perpetual war: lessons from nature. IEEE IT Professional, vol. 17, no. 1, pp. 16-22, January/February 2015

[3]Hofmeyr S A, An Immunological Model of Distributed Detection and Its Application to Computer Security, Ph.D. Thesis, University of New Mexico, 1999.

[4]Zou C C, Gong W, Towsley D, Gao L, The monitoring and early detection of internet worms, IEEE/ACM Transactions on Networking (TON) 13 (5) (2005) 961–974.

[5]Ford R, Bush M, Bulatov A, Predation and the cost of replication: New approaches to malware prevention?, Computers & Security, Volume 25, Issue 4, June 2006, Pages 257-264

[6]Crandall J R, Ladau J, Ensafi R, Shebaro B, Forrest S, The Ecology of Malware, Proceedings of the New security paradigms Workshop (NSPW '08), pp. 99-106, Lake Tahoe, CA, USA.

[7]Blumstein D T, Fourteen lessons from anti-predator behaviour, In: Natural security: A Darwinian approach to a dangerous world (R. Sagarin and T. Taylor, eds.). U. California Press, 147-158, 2008.

[8]Okhravi H, Hobson T, Bigelow D, Streilein W. Finding Focus in the Blur of Moving-Target Techniques. IEEE Security & Privacy, vol.12, no. 2, pp. 16-26, Mar.-Apr. 2014

[9]de Castro, L. N., & Von Zuben, F. J. (2000). The clonal selection algorithm with engineering applications.In Genetic and Evolutionary Computation Conference (GECCO) (pp. 36-37). Las Vegas, USA

[10]Greensmith, J. (2007). The dendritic cell algorithm, PhD Thesis, University of Nottingham, UK.

[11]Hart, E., &Timmis, J. (2008). Application areas of AIS: The past, the present and the future. Applied Soft Computing, 8, 191-201.

[12]Fink, G.A.; Haack, J.N.; McKinnon, A.D.; Fulp, E.W., "Defense on the Move: Ant-Based Cyber Defense," Security & Privacy, IEEE , vol.12, no.2, pp.36,43, Mar.-Apr. 2014

[13]Sean P. Gorman, Rajendra G. Kulkarni, Laurie A. Schintler, and Roger R. Stough. 2004. A predator prey approach to the network structure of cyberspace. In Proceedings of the winter international synposium on Information and communication technologies (WISICT '04). Trinity College Dublin 1-6.

[14]Kephart J, White S. Measuring and modeling computer virus prevalence. In: Proceedings of the 1993 IEEE computer society symposium on research in security and privacy, Oakland, California; May 24–25, 1993. p. 2–14.

[15]Romualdo Pastor-Satorras and Alessandro Vespignani, Epidemic Spreading in Scale-Free Networks, Phys. Rev. Lett. 86, 3200, April 2001

[16]HoomanMohajeriMoghaddam, Baiyu Li, Mohammad Derakhshani, and Ian Goldberg. 2012. SkypeMorph: protocol obfuscation for Tor bridges. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 97-108

[17]G. D. Ruxton, T. N. Sherratt, , and M. P. Speed. Avoiding Attack: The Evolutionary Ecology of Crypsis, Warning Signals and Mimicry.Oxford University Press, 2004.

[18]E. Zielinska, W. Mazurczyk, K. Szczypiorski - Trends in Steganography - Communications of the ACM, vol 57, No.2, March 2014, pp. 86-95

[19]Stenseth N.C., Smith J.M. 1984. Coevolution in Ecosystems: Red Queen Evolution or Stasis? Evolution 38(4): 870-880.

[20]Moore P.S., Boschoff C., Weiss R.A., Chang Y. 1996.Molecular Mimicry of Human Cytokine and Cytokine Response Pathway Genes by KSHV. Science, 274(5293): 1739-1744.

[21]How MJ, Zanker JM. 2014. Motion camouflage induced by zebra stripes. Zoology. 117(3): 163-170.

[22]Delves P.J., Martin S.J., Burton D.R., Roitt I.M. 2011. Essential Immunology.Wiley-Blackwell.

[23]Krebs C.J. 2009. Ecology: the experimental analysis of distribution and abundance. Bejamin Cummings, San Fransisco, USA.

[24]Rooney N, McCann KS. 2012. Integrating food web diversity, structure and stability. Trends in Ecology and Evolution, 27(10: 40-46.

[25]Ings TC. Et al. 2009. Review: Ecological networks – beyond food webs. Journal of Animal Ecology 78(1) 253-269.

[26]Axelrod R, Hamilton WD. 1981.The evolution of cooperation. Science, 211(4489): 1390-1396.

[27]Riolo RL, Cohen MD, Axelrod R. 2001. Evolution of cooperation without reciprocity. Nature 414: 441-443.

[28]Andersson M. 1995. Sexual selection.Princeton University Press.

[29]NeffBD, Pitcher TE. 2005. Genetic quality and sexual selection: an integrated framework for good genes and compatible genes. Molecular Ecology, 14(1): 19-38.

[30]Miner BG, Sultan SE, Morgan SG, padilla DK, Relyea RA. Ecological consequences of phenotypic plasticity. Trends in Ecology and Evolution 20(12): 685-692

[31]Whorf BL. Language, thought, and reality: selected writings of Benjamin Lee Whorf. In: Carroll JB, editor. Cambridge, MA: MIT Press; 1956

[32]R. Raffel, L.B. Martin, J.R. Rohr. 2008. Parasites as predators: unifying natural enemy ecology. Trends in Ecology and Evolution 23(11): 610-618.

[33]T. Royama. 1971. Comparative study of models for predation and parasitism. Researches of Population Ecology 13(Supp 1): 1-91.

[34]M.F. Benard. 2004. Predator-induced phenotypic plasticity in organisms with complex life histories. Annual Review of Ecology Evolution and Systematics 35: 651-673.

[35]R. Sorek, V. Kunin, P. Hugenholtz. CRISPR — a widespread system that provides acquired resistance against phages in bacteria and archaea. Nature Reviews Microbiology 6: 181-186.

Author Detail's:

Dr Ramana (Naik) Banothu

A warded Ph.D from SC&SS, JNU, New Delhi in data mining. Working as Professor & Principal Trinity Engineering College, Pedapalli Dist., Telangana State; He is fellow member of international and national level professional bodies and he is a reviewer for peer reviewed journals. His areas of interest are Computer Graphics, Data Mining, Artificial Intelligence. He represented for Indian Delegate & presented paper on topic "Youth Role in World Peace" at16th World Youth Festival Venezuela 2005 @ Caracus. He is a Member in Fellow FIE, Institute of Engineers (India),OUCIP – Osmania University Centre for International Programmes, (Previously called as ASRC – American Studies Research Centre); Computer Society of India (CSI); Institute of Constitutional & Parliamentary Studies (ICPS), VP House, New Delhi; Osmania Graduates Association (OGA).