Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments

Reza Montasari, Amin Hosseinian-Far and Richard Hill

Abstract Despite the increasing evolution of the cyber environment, enterprises seem to find it challenging to identify a solution to create an effective defensive posture. As the cyber phenomenon becomes a fundamental part of our society, it is essential to identify adaptive methods to increase the worldwide defensive condition in the most effective manner possible. A decade ago, it was not possible to imagine todays cyber-threat landscape. Cybercriminals have adapted their methods to circumvent traditional defences and hide undetected on systems for months or even years. There are different reasons for such attacks, and understanding the psychology of attacks are essential. Therefore, enterprise security also needs to be adapted with an intelligence, multi-layered approach to IT security. This paper surveys the latest research on the foundation of Adaptive Enterprise Security (AEC). To this end, it discusses potential security policies and strategies that are easy to develop, are established, and have a major effect on an enterprises security practices. These policies and strategies can then efficiently be applied to an enterprises cyber policies for the purposes of enhancing security and defence. Moreover, it will take into briefly discuss the need for a thorough understanding of human factors and psychology of attacks. The study also discusses various adaptive security measures that enterprises can adopt to continue with securing their network and cyber environments. To this end, the paper continues to survey and analyse the effectiveness of some of the latest adaptation techniques deployed to secure these network and cyber environments.

Reza Montasari
Birmingham City University, School of Computing and Digital Technology, Birmingham, B4 7XG, UK, e-mail: Reza.Montasari@bcu.ac.uk

Amin Hosseinian-Far
University of Northampton, Department of Business Systems & Operations, Northampton, NN2 7AL, UK, e-mail: Amin.Hosseinian-Far@northampton.ac.uk

Richard Hill
University of Huddersfield, Head of Department of Computer Science, Huddersfield, HD1 3DH, UK, e-mail: R.Hill@hud.ac.uk

1 Introduction

In today′s cyber security environment, there is a growing number of threats resulting from old and new sources. The speed, diversity and frequency of such attacks are generating cyber security challenges that have never been witnessed before [15]. Moreover, the essence and purpose of the attacks are evolving in that they are becoming more politically and economically motivated [15, 21]. Several critical infrastructures such as industrial control systems are attractive targets for cyber-attacks [29]. Therefore, identifying, assessing and protecting assets and resources from harm are of utmost importance [18]. With the increasing number of new types of attack techniques such as zero-day exploit attack and advanced persistent threats, network security is encountering severe ”easy-to-attack and hard-to-defend” challenges [17, 25]. Adversaries have time benefit to scan and acquire information on targeted systems before carrying out attacks. The longer an attacker is within a system, the more difficult it is for the cyber-defenders to contain and expel them from their cyber domain. The more time the attacker has, the safer environments they can create and hide within them. They can install modified backdoors to dominate and threaten network systems after vulnerabilities have been discovered through the benefits of asymmetric information.

As enterprises of different sizes encounter rapidly growing frequency and sophistication of cyber-attacks, such threats have had detrimental effects on network security, compliance, performance, and availability. Moreover, many of such threats have eventuated in the theft or exposure of sensitive data. A cyber-attack can have devastating effect on an enterprises viability, and the results of such attacks can have lasting impact on its brand with negative long-standing effects on customer trust and loyalty. Many victim organisations have also experienced collateral damages including: fines, lawsuits, credit problems and reduced stock prices. The public revelation resulting from a breach goes beyond the IT realm, affecting every aspect of business within the organisation. Advanced Persistent Threats (APTs), sophisticated malware and targeted attacks are some of the new, constantly evolving threats that enterprises face when searching for cracks in enterprise IT systems. Various enterprise technologies such as smart mobile devices, web applications, portable storage, virtualization, cloud-based technologies present cybercriminals with convenient support network of attack vehicle.

At the same time, many systems are developed with set limits and presumptions without the capability to adapt when assets change suddenly, new threats emerge or unfound vulnerabilities are exposed [48]. The features offered by the existing defence methods are not capable of determining all kinds of network attacks to protect systems proactively [32]. Current defence methods such as firewalls and intrusion detection systems are always behind adversaries sophisticated exploitation of systems susceptibility. The existing cyber defences are mainly static and are administered by slow processes such as testing, security patch deployment and also human-in-the-loop monitoring. Consequently, attackers can methodically explore target networks, premeditate their attacks, and continue for a long time inside compromised networks and hosts with an assurance that those networks will change slowly. This is due to the fact that hosts, networks and services that are mainly developed for the purposes of availability and uniformity do not reconfigure, adapt or regenerate apart from ways to support maintenance and uptime requirements.

Many systems are developed with set limits and presumptions without the capability to adapt when assets change suddenly, new threats emerge or unfound vulnerabilities are exposed. Thus, in order to address such changes, systems must be developed such that they are capable of enabling various security countermeasures dynamically [48]. Moreover, to tackle cyber-security threats more effectively, enterprises will also need to have more robust cyber security policies and systems that will enable the reinforcing of the defence and make the cyber-defenders more effective when responding to attacks. In addition, enterprises will need to have a new, more adaptive, integrated approach based on the foundations of prediction, prevention, detection and response so as to address the limitations of traditional enterprise IT systems security. Such robust policies and systems must be developed and updated to facilitate various security countermeasures dynamically.

This paper surveys the latest research on the foundation of Adaptive Enterprise Security (AEC). To this end, it discusses potential security policies and strategies that are easy to develop, are established, and have a major effect on an enterprises security practices. These policies and strategies can then efficiently be applied to an enterprises cyber policies for the purposes of enhancing security and defence. The study also discusses various adaptive security measures that enterprises can adopt to continue with securing their network and cyber environments. To this end, the paper continues to survey and analyse the effectiveness of some of the latest adaptation techniques deployed to secure these network and cyber environments.

The remainder of this paper is structured as follow: The next section, Section 2, discusses potential security policies and strategies that have a major impact on an enterprises security practices. Section 3 discusses various adaptive security measures, while Section 4 surveys and analyses some of the latest adaptation techniques employed to secure network and cyber environments. The final section, Section 5, presents the conclusions. Two main contributions of this paper are the scope of the discussion no surveys of similar scope currently exist and the provision of a research agenda focused on security matrix for adaptive network and cyber security.

2 Security Policies and Strategies

In situations where an enterprise needs to develop a more effective cyber defence stance, there will be a priority of work that must be undertaken to ensure achievement. The first phase for an enterprise is to establish a robust governance that employees will adhere to and trust. In order to accomplish this, the main leadership within an enterprise must engage in the cyber defence governance panel. The high-ranking officials agreeing and signing off on decisions will highlight to the employees the significance of the cyber defence to the enterprise [15]. Such approach will also enable the employees to remember that the cyber threat is always present and that the safeguarding measures are supported by the high-level leadership.

The second phase in developing a robust governance model must include a vigorous training. There already exist many Good Practice Guides providing the details on how to create a new or improve existing cyber awareness and skills for enterprise systems [47, 45, 52, 4, 12, 54]. These documents often place a high emphasise on the frequency and consistency of the training. Such guides enable employees to perform in accordance with established security policy and to report incident with confidence that they are doing the right thing at the right time. Moreover, creating a robust governance requires the development of some kinds of a recognition system whereby employees are rewarded for the fact that they have acted responsibly to stop incidents or attacks or any other exploits that enhances the defence of the enterprise [15].

The second priority of actions for the enterprise must be the collection, processing, and distribution of actionable intelligence to the companys cyber defence team. Assessing the laborious task of selecting and establishing relationships at the early stage will be valuable to the enterprise in the long run. There will be various sources of information and partners that an enterprise should search for. External sources consist of agencies such as the UK National Cyber Security Centre, which is the governmental agency that helps networks of national significance and all sectors of industry against sophisticated attacks [42], the wider public sector and academia. Some of the services offered by the NCSC include helping the enterprises:

- determine the extent of the incident,
- work to ensure the immediate impact is managed,
- provide recommendations to remediate the compromise and increase security across the network,
- produce an incident report to describe the scope of the problem, the technical impact, mitigation activities and an assessment of business impact, and
- give an Impact Assessment where the incident affects partners or customers.

Enterprises should also have a policy of creating a relationship with law enforcement agencies that are responsible for cybercrime. In some cases, if possible, the enterprises cyber governance panel must also provide a seat for a law enforcement liaison to participate. Such liaison will assist with providing a consistent direction from the enterprises direction and will facilitate and accelerate communications in case of attacks [15]. Then, there need to be (within the Service Level Agreement (SLA) between the company and their ISP agreements on communication lines) information allocation, and accountabilities during the periods of disaster. For instance, this should cover the actions to be taken to ensure business continuity and disaster recovery. Nowadays, enterprises are increasingly adopting cloud services that necessitate some kinds of SLA with the cloud service provider.

In the final phase, there must be a robust policy to create information dissemination amongst the enterprise and other companies within the same industry or companies that deploy identical IT equipment. In such relational situations, enterprises, however, will need to balance out issues such as complying with Intellectual Property and at the same time, also maintaining competitive advantage even if they are disseminating information of cyber-attacks. Sharing information on cyber-attacks is economically valuable to both parties. An example of such cooperation between different enterprises is of that between the auto and financial industries by developing joint Cyber security centers [15].

The most effective way to distribute information while protecting Intellectual Property is to adopt a standard to exchange information such as STIX and TAXII [57]. The most excellent source of information is often within the enterprise, themselves. This consists of the IT infrastructure and employees. The acquisition and examination of logs and their behaviour are vital in establishing an effective cyber security stance and a swift and robust cyber defence response. Collecting intelligence from employees is also essential; for instance, employees must be asked to report malevolent emails or social engineering attempts. Also, providing employees with instructions on reporting mechanism must become part of the security awareness training within the enterprise. Such training must cover (1) what to report, (2) when to report, and (3) whom to report to [15]. Publically providing employees with awards in situations where they have operated according to the training enhances such actions. This is highly likely to lead to more participation of the employees, in turn resulting in the formation of impetus and enthusiasm for cyber security amongst the employees.

The final decision associated with intelligence gathering is the execution of a system that will collect, organise, combine, and conduct an initial examination of all the acquired information. Such a system can function as an intelligence. Nevertheless, the technology will be extraneous as long as there is a systematic approach with a feedback mechanism to the formation of intelligence that will enable the cyber-security team to detect and prevent an intrusion, find the intruders, and react to safeguard the system in a speedier manner and with more precision. The next policy decision must be about the size of the cyber-security team that an enterprise requires to safeguard a robust defence that is capable of both preventing and reacting effectively. Godin (2017) suggests the ratio of $20-25$ per 1000 employees and IT equipment combined [15]. For instance, an enterprise with 10000 employees and 15000 pieces of IT equipment (25000 combined) will require a cyber-security team of 500 to 625. This team will consist of system administrators, service desk personnel, technicians, and Cyber security experts.

However, it should be noted that an enterprise cannot be expected to terminate all nefarious activities in their network or cyber space. However, there exist steps that an enterprise can undertake to assure that they are not part of the problem. When attempting to use the principles of neutralisation, the major effort must be placed on splitting the connections amongst the attackers systems. To this end, two measures will need to be adopted. The first measure is to ensure that there does not exist a link between the attackers systems by acting as a node or a transit point. The policies discussed previously will enable enterprises to ensure that their network and cyber domains do not become a refuge for cyber-criminals [3, 15]. The second measure is to carry out a supply chain analysis to ensure its integrity. Such measures will enable the enterprises to avoid providing refuge or resources to cyber-criminals [41, 36].

3 Adaptive Security Measures

Security requirements is about extracting, representing and examining security goals and their relationships with other security elements such as critical assets, threats, attacks, risk, and countermeasures [43, 48, 39]. However, such elements can dynamically change as the functioning environment or the requirements change. Unfortunately, current security requirements engineering techniques are not capable of identifying and dealing with runtime changes that particularly affect security [5]. Therefore, adaptive security is needed to address such runtime changes. The main goal of an adaptive security is to identify and analyse different kinds of changes at runtime that might have a negative impact on system security and activate countermeasures offering an acceptable level of protection [46, 43]. For instance, integrating a valuable asset into the system might require a higher level of protection which in turn demands stronger countermeasures. Security objectives might change, new threats and attacks might arise, new system vulnerabilities might be found, and current countermeasures might become ineffective. In such situations, adaptive security must be capable of addressing the impacts of such changes, which might undermine the system and harm its resources [48].

When designing and implementing adaptive security systems, three main models must be considered. These include Asset Model, Objective Model, and Threat Model [1]. The Asset Model signifies assets and their relationships [39]. In the context of a network, assets signify individual nodes on the network, such as servers, routers, and laptops. Asset ranges signify a group of network nodes addressable as adjacent block of IP addresses. Zones signify allocations of the network itself and are also defined by an adjacent block of addresses. The attacks that target a network might damage or impair the connected assets as well.

On the other hand, the Objective Model signifies the main goals which a system must attain and disintegrates them into functional and non-functional requirements. Such a model consists of security objectives including Confidentiality, Integrity, Availability and Accountability (CIAA) [48]. Security objectives consist of a hierarchical structure and can be disintegrated into operational countermeasures which include various operations to alleviate security risks [39, 51]. Some security objectives cannot be satisfied without sacrificing other non-functional requirements such as performance and usability [48]. The countermeasures used to impose the satisfaction of security objectives cannot be chosen without taking into account their side effects. For instance, if a system deploys a higher level of encryption algorithm, such countermeasure might create deterioration in system performance or usability. Similarly, a threat model consists of threat agents, threat goals, and attacks. Threat agents can be natural (e.g., flood), human (e.g., hacker), or environmental (e.g., power failure) [48, 51, 19]. Assets are associated with the threat objectives that they inspire, whereas threat objectives are connected with the attacks that are carried out for their attainment. Threat objectives signify motivations of threat agents to attack a system [48]. Attacks are activities whereby threat goals can be attained and as a result assets would be harmed [43, 31, 51]. Thus, threats can be modelled as ”operationalizations of threat goals” [48].

Often, it is difficult to ascertain the security of the design process of network systems resulting in security weaknesses. In addition, the static implementation of the current network information systems presents the attackers with adequate time to scan and identify systems vulnerability. Thus, it will be increasingly challenging for the traditional static defence systems effectively to withstand unknown system hardware and software weaknesses, and to avert possible backdoor attacks and the growing sophisticated and intelligent network intrusion penetrations. Therefore, such a situation aggravates the asymmetry between the offense and the defence in the network. A new technology titled Adaptive Cyber Defence (ACD) challenges attackers with changing attack surfaces and system configurations, compelling attackers constantly to re-evaluate and revise their cyber activities. Despite the usefulness of technologies such as Moving Target Defence, Dynamic Diversity, and Bio-Inspired Defence (discussed later in the paper), all these technologies presume static and aleatory but non-adversarial environments [7]. Cybenko et al. argue that in order to reach full potential, scientific foundations need to be developed in order for system resiliency and robustness in adversarial environments to be rigorously defined, quantified, measured and extended in a laborious and reliable manner [7].

Therefore, by countering an attack in a timely fashion, an adaptive security aims to reduce the effect and extent of potential threats. This consists of the possibility of responding to ”zero-day” attacks, in which a threat is so new that there does not yet exist a patch or other countermeasure. Despite the fact that adaptive security measures are evolving, an adaptive method can be developed by utilising technologies available today. This remainder of the section presents concepts related to adaptive security and the manner in which the method enhances system survivability. It discusses adaptive security and the reason why the method is beneficial, reviews its features and principles, and also discusses a design approach. To this end, this section addresses the following topics:

1. Objectives and Components of Adaptive Security,
2. Complex Adaptive Systems in Security Design,
3. Structural Approach Based on Adaptive Security, and
4. Design Approach to an Adaptive Security Model.

3.1 Objectives and Components of Adaptive Security

In the context of IT infrastructure and cyber-security, an Adaptive Security approach aims to contain active threats and also counterpoise potential attack vectors. Similar to other security architectures, Adaptive Security Model aims:

- to decrease threat intensification and limiting the potential dissemination of failures,
- to make the target of an attack smaller,
- to reduce the rate of attacks,
- to respond to an attack quickly,

- to stop attacks that attempt to restrict resources, and
- to address attacks aimed at compromising data or system integrity.

Furthermore, in addition to supporting SLAs, the main aim of an adaptive security approach is to maintain system and data integrity, facilitate reliability and assurance. Similar to all other types of security approaches, the adaptive security ultimately is aimed at ensuring that data and processing resources are trustworthy, reliable, available, and functioning within satisfactory boundaries. Also, one of the main principles of the adaptive security is survivability which is the ability of a system to accomplish its mission in a timely way when attacks, failures and accidents take place [35]. In order to ensure the survival of a system, it is imperative first to distinguish system elements (i.e. things that must survive) against elements that are considered sacrificial. For the purposes of this paper, a system is deemed to have survived if it endures to accomplish its business goals within planned Service Level Agreements (SLAs) [62]. An Adaptive Security Architecture encompasses four crucially important capabilities as depicted in Figure 1 [58, 35].

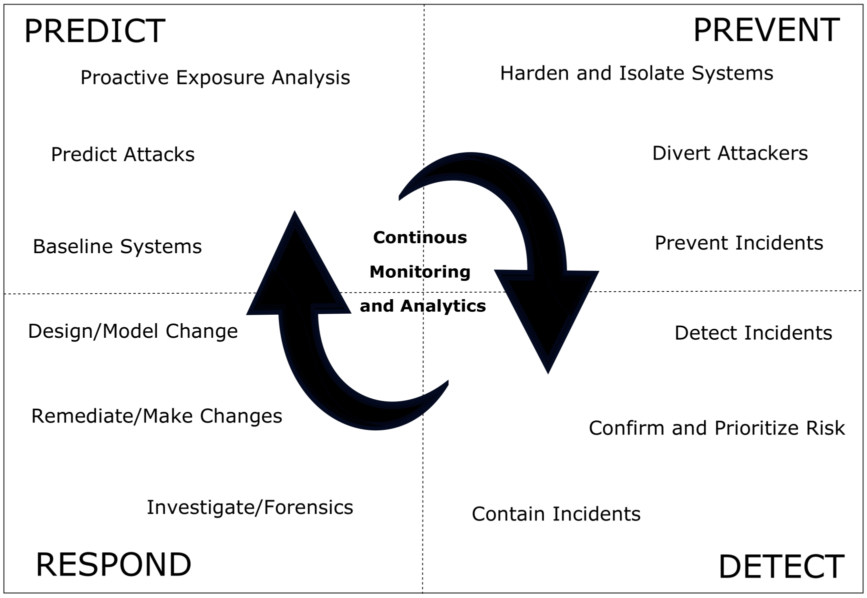

Fig. 1 Adaptive Security Architecture, Adapted from MacDonald and Firstbrook (2014) as cited by Vectra (2016) [35, 58]

Prediction: Those enterprises that have access to the latest threat intelligence and trends are better equipped to predict and avoid attacks. Training employees to distinguish tactics deployed in attacks boosts prognostic analysis in addition to the capability to learn from past mistakes by forensically examining breaches

[22, 23]. Moreover, penetration testing can also assist with revealing the weak spots in enterprises IT systems security.
Prevention: The main goal of prevention will be to diminish attack surface regardless of the attack being traditional, signature-based anti-malware, device controls or patching application vulnerabilities. Tightening systems and deploying as many as hurdles in the way of attackers as possible are two main aspects of an all-embracing approach that includes restricting the capability of attacks to propagate and decrease their impact.
Detection: Advanced attacks can remain undetected for many months and even years. According to a research conducted by Kaspersky Lab (2016), some attacks can remain undetected up to 200 days [28]. Technologies for incident detection underlined by the best threat analysis enhances incident detection. The most effective detection strategy is often developed based on the capability to figure out behaviours and sequences of events that indicate a breach has occurred.
Response: Efficient enterprise security should include the capability to respond to and reduce the effects of a breach. This can include: (1) ”if/then” policy for procedures that can be automated such as patching, and (2) post-breach examination or the utilization of incident-response expert teams to halt, reduce and investigate attacks, breaches and other security incidents. In order to be effective, these capabilities must work together as a multi-tiered system. Some of the main attributes of an all-inclusive, adaptive enterprise security architecture are intelligence-driven, threat focused, integrated, holistic and strategy-driven.

3.2 Complex Adaptive Systems in Security Design

Complexity is the major barrier in designing secure IT architectures and effectively fighting security threats. Complex systems are not understood by anyone. Therefore, if no one can comprehend more than a portion of a complex system, then no one can foresee all the ways that a system can be penetrated by an attacker [62, 11, 14]. Averting insecure operating modes in complex systems is challenging and unlikely to do without incurring a significant cost. This denotes that the defenders or enterprises have to counter all possible attacks; the attacker only needs to identify one insecure means of attack. A potential solution to the increased complexity of IT security infrastructure is a Complex Adaptive System, which is an active network of various distributed and decentralized agents that continuously interrelate with and learn from one another. A security architecture that impersonates a Complex Adaptive System can be efficient in that it can adapt and respond continuously to emerging and changing security threats.

3.3 Structural Approach Based on Adaptive Security

In order to detect threats effectively, IT systems will need to understand a baseline of what is deemed normal behaviour and what is not considered normal. The notion of self and non-self are central in IT systems. Functional systems effectively distinguish between what is native to the system and what is not native. What is not native is considered as a threat and eradicated. An IT system is automatically capable of safeguarding itself by accurately detecting and dealing with threats and suspicious activity and differentiating these from legitimate components, protocols and operational processes within IT infrastructure. An IT infrastructure intended for survivability must present the following characteristics [62, 26]:

- The flexibility to respond to new and diverse threats,
- The capability of being self-detecting, self-governing, self-recovering and self-protecting,
- A basis on a formalised security model with enforcement mechanisms that enforce security policy compliance,
- The ability to identify unauthorised resource modification such as data, files, file systems, operating systems and configurations, and also launch remedial actions such as (a) quarantining resources for the purposes of digital forensic investigations so that the system can learn from the attack, and (b) providing other resources to substitute for compromised systems in order to facilitate service continuity, and
- Applying remedial actions as required.

Adaptive security takes advantage of architectural and operational principles from different disciplines. The following principles are applicable to information systems. These principles are identified [27, 62, 64, 26, 9] as valuable features that are valuable in IT systems to decrease exposure to threats, contain the degree of threats and fight them in a timely manner.
Pattern Recognition: IT systems need to be able to address sophisticated pattern matching techniques in order to detect regular and irregular behaviour in code, command/response dialogues, communication protocols, etc.
Uniqueness: IT systems need to be able to address sophisticated pattern matching techniques in order to detect regular and irregular behaviour in code, command/response dialogues, communication protocols, etc. Uniqueness discourages the existence of monocultures that can be vulnerable to a common computer virus. It also equips diverse IT systems with the essential robustness to survive targeted threats.
Self-Identity: IT systems isolate and eliminate what does not belong according to baseline manifests and security policy. This includes support for intra/inter-systems communication and sharing information on threats, countermeasures, security policies, and trust relationships between systems and IT infrastructure.
Diversity: In IT systems, diversity displays itself through various control mechanisms such as compartmentalization through operating system virtualization of Trusted Platform Module (TPM)-based hardware trust anchors [62].

3.4 Design Approach to an Adaptive Security Model

An automatic system that integrates an insusceptible response ability could be a reasonable design approach in developing a secure Adaptive Security Model. One way of utilising adaptive principles is through Defence-in-Depth security architecture that implements various strategies. Diversity can be accomplished by applying mechanisms such as clustering, redundant hardware or numerous kinds of firewall appliances from multiple vendors. In this method, if one components fails to respond to a certain threat, it is probable that other components do not capitulate. In this way, the survivability of the system is preserved. Similarly, the property of elasticity can be maintained via virtualization techniques. Employing virtualization technologies, infrastructure systems can categorise various system services in secure execution containers. These containers can be deployed to separate service instances. This denotes that if a threat alters a service in one container, it will not affect the implementation of running services in other containers. This will ensure that services within IT infrastructure can continue.

At the same time, response mechanisms could quarantine the affected container and contain the attacks impact. The main difference in an adaptive security architecture from the existing state-of-the-art practices is that adaptive security approaches are implemented not only to defend against known threats but also to predict unknown threats [27]. The following outlines one possible way of implementing an adaptive security architecture in both cyberspace and network security environments. This method should be incorporated into a larger context of the complete security architecture. Moreover, it must take place within the framework of other security features such as application, system, network design, and quality assurance and configuration validation to assure that all components and design elements adhere to the overall security policy [62].

The followings provide an outline of the steps required to design and implement an adaptive security model [27, 62, 26, 9]:

- Delineate threats and its features that are necessary to avoid or destroy. A threat feature is likely to comprise the entire threat structure. It could also be a specific activity displayed by an entity or process.
- Ascertain satisfactory behaviour, trusted components and activities that must be differentiated from a threat. This step is crucial to stop Denial-of-Service (DoS) attacks.
- Characterise triggers that could scan for suspicious activities and to launch threat detection sensors that will warn the larger IT infrastructure of possible threats and prepare threat response mechanisms.
- Carry out redundancy for main functions.
- Describe threat response mechanisms that do not culminate in terminating the host.
- Outline a recovery process through which systems are able to reconfigure and restart themselves adaptively. This process must also consist of a learning and

knowledge dissemination mechanism in order for infrastructure to learn how to evade analogous threats in the future.

- Outline feedback abilities that will enable the threat response mechanism to authenticate threats in order for them to respond only to valid and realistic threats. Such feedback mechanisms assist with ensuring that the triggers and threat response mechanisms recognise the security setting within which they function. This will facilitate the preferred adaptive behaviour.

Not every infrastructure should have every threat features delineated. The purpose should be to develop a varied set of systems, each of which can have different threat response abilities. By filling the fundamental building blocks of threats and threat responses, individual systems will be capable of adapting to threats and respond to these threats accordingly. Once the response is successful, the individual system can then disseminate that knowledge with other reliable systems that have not undergone the original threat. It is expected that sacrificial components are implemented into the complete IT infrastructure. Thus, a threshold of acceptable harms should be established and monitored.

4 Adaptation Security Techniques

As stated previously, current cyber defences are mainly static providing adversaries with opportunities to probe the targeted networks with the assurance that those networks will change slowly, if at all. Often, adversaries are not concerned with time to develop reliable exploits and premeditate their attacks since their targets are static and almost undistinguishable [7, 60]. In order to address such situations, researchers in the domain of security have started to explore different approaches that make networked information less analogous and less predictable [2, 55, 60, 8, 7, 24, 25]. The main reason for Adaptation Techniques (AT) is to design systems with similar functionalities but randomised manifestations. Adaptation methods are normally deployed to deal with various phases of potential attacks [7]. In contrast, various defence undertakings could have various Confidentiality, Integrity, Availability and Accountability (CIAA) requirements [48]. For instance, if a cyber-attack on Availability were assessed to be present or imminent, adaptation mentors for preserving availability would be given priority over methods for improving confidentiality or integrity. Analogous functionality enables authorised usage of networks and services in predictable, formal ways at the same time that randomised manifestations make it cumbersome for adversaries to develop exploits remotely. Preferably, each exploit would need the same amount of the effort by the adversary. The remainder of this section aims to survey and analyse some of the latest Adaptation Techniques proposed by the research community. This examination has been restricted to only six techniques due to the space constraints.

Instances of the Adaptation Techniques (AT) include the following notions to the degree that they implicate system adaptation for security and resiliency purposes [2, 55, 8, 7, 24, 25]:

- Randomized Network Addressing and Layout,
- Network Moving Target Defence (MTD),
- Inference-Based Adaptation,
- ACD Framework Based on Adversarial Reasoning,
- OS Fingerprinting Multi-Session Model Based on TCP/IP, HTTP and TLS,
- Address Space Layout Randomization,

4.1 Randomized Network Addressing and Layout

Randomized instruction set and memory layout restrict the degree to which a single buffer overflow based penetration could be utilised to breach a collection of hosts. This, however, at the same time, makes it more challenging for cyber-defenders (e.g. systems administrators or software developers) to debug and update hosts due to the fact that all the binaries are different. Additionally, randomised instruction set and memory layout techniques will not present the adversaries with a difficult challenge to determine a networks layout and its available services. Analogous examination can be carried out for each of the above techniques. For instance, randomising network addresses will present attackers with more challenges to conduct reconnaissance on a target network remotely. However, it does not create any difficulty for the adversary to penetrate a particular host after it has been identified and reachable. Another example can relate to that of a mission such as the generation of a daily Air Tasking Order (ATO) [7], which could prioritize confidentiality and integrity to safeguard details of future sorties over availability in order for the network layout and addressing to be used to perplex potential adversary at the expense of network performance.

4.2 Network Moving Target Defence

Network Moving Target Defence (NMTD) is employed to enhance the efficiency of defensive mode and facilitate a dynamic, non-deterministic and non-sustained runtime environment [32, 53, 24, 25]. The NMTD is an innovative Adaptation Technique that changes the adversarial patterns amongst attack and defence with an endpoint information hopping. It disrupts the dependency of the attack chain on the consistency of the network operating environment by multi-level dynamical changes [32]. One of the significant elements of the NMTD is the Endpoint Hopping Techniques, which have received extensive attention [32, 65]. Although such techniques are useful, they do not enable the full potentials of NMTD hopping resulting in limiting their use in simple network threat such as APT and zero-day attacks.

There exist two main issues with the existing end-point hopping research. The first significant problem is that the advantages from hopping defence is reduced because of the insufficient dynamic of network hopping triggered by self-learning inadequacy in reconnaissance attack strategy culminating in the blindness of hopping mechanism selection. The second main problem is that because of the restricted network resources and high overhead, the availability of hopping mechanism is low. Thus, to address such issues, Network Moving Target Defence based on Self-Adaptive End-Point Hopping Technique (SEHT) has been proposed [32]. The SEHT was developed to address the lack of hopping mechanisms capable of self-adaptive to scanning attacks, and also to describe the restraints of hopping formally which increases the availability of hopping mechanisms in order to ensure the low hopping overhead. The SEHT is claimed to be capable of counterweighing the defensive value of end-point information hopping and service quality of network system, based on adversary strategy awareness.

Through their theoretical and experimental results reported in their research paper, it appears that Lei et al. (2017) have addressed the blindness issue of hopping mechanism associated with defence by applying hopping triggering based on adversary strategy awareness [32]. The aim of this solution is to direct the choice of hopping mode by discriminating the scanning strategy, which improves targeted defence. Lei at al. (2017) also employ ”satisfiability modulo” theories to describe hopping constraints formally in order to ensure low hopping overhead [32].

4.3 Inference-Based Adaptation

Inference-Based Adaptation techniques focus on tackling stronger attacks in wireless communications where observant attackers can attain significant gains by incorporating knowledge of the network under attack. In these situations, cyber-criminals are capable of adapting parameters and behaviours to offset system dynamics, hinder detection, and save valuable resources. Thus, robust wireless communication protocols that can survive such adaptive attacks require new techniques for near-real-time defensive adaptation, allowing the defenders similarly to change their parameters in response to perceived attack impacts. One of such latest new techniques is Inference-Based Adaptation Techniques for Next Generation Jamming and Anti-Jamming Capabilities [8, 55].

4.4 ACD Framework Based on Adversarial Reasoning

ACD framework that deploys adversarial reasoning is aimed at dealing with several limitations of traditional game-theoretic analysis such as empirically defining the game and the players. The framework utilises control-theoretic analysis to bootstrap game analysis and to quantify the robustness of candidate actions [7]. This framework comprises of four parts, each of which has a different purpose. The aim of Part 1 is to design and implement a subsystem which takes two inputs including streaming observations of the networked system and also external intelligence about possible adversaries. The purpose of Part 2 is to employ empirical methods to activate a game model from which it acquires ”strategically optimised defence actions”. The goal of Part 3 is to focus on identifying and adding innovative adaptation mechanisms into the defence strategy space. Part 4 aims to conduct trade off analysis which will consider not only functionality, performance, usability and exploitation but also robustness, stability, observability and resilience.

4.5 OS Fingerprinting Multi-Session Model Based on TCP/IP, HTTP and TLS

Enterprise networks encounter various menace activities such as attacks from external devices [6], contaminated internal devices [59] and unauthorized devices [17, 61]. One important traditional method of defence is Passive Operating System Fingerprinting (POSF), which detects the operating system of a host merely through the observation of network traffic. POSF discloses vital information such as intelligence to the defenders of heterogeneous private networks. Meanwhile, cyber-criminals can employ fingerprinting to explore networks. Therefore, cyber-defenders require obfuscation techniques to thwart these attacks. POS Fingerprinting techniques emerged almost two decades ago in order to deal with remote devices sending network attack traffic [50]. As a result it was quickly adopted by the open source community [66]. Subsequently, research community built upon Passive OS Fingerprinting further. For instance, Lippmann et al. (2003) as cited by Anderson and McGrew (2017) presented the notion of Near-Match Fingerprints, employed machine learning classifiers to produce them, and ascertained the OS groups that were distinguishable through fingerprinting [33, 2]. Tyagi et al. (2015) deployed passive OS Fingerprinting of TCP/IP to identify unauthorized operating systems on private internal networks [56].

The data structures originally employed in fingerprinting originated from TCP/IP headers. However, the latest research has applied characteristics from HTTP headers [40, 66] and unencrypted fields from the TLS/SSL handshake [10, 20]. These characteristics can be examined independently when only a single sessions data is available, which is not unusual in some scenarios. Despite the fact that it is valuable for cyber-defender (e.g. network administrators) to apply Passive Fingerprinting to detect operating systems on their networks, cyber-criminals have also adopted these techniques to seek for possible victims [2]. Due to the fears resulting from malevolent use of detection, cyber-defenders have attempted to identify new methods to apply obfuscation to overcome the technique. Although these techniques have been useful in that that are capable of obscuring individual session or raw data structures that a cyber-defender controls; nevertheless, they are less ineffective in the multi-session model. This is because it is unusual for a cyber-defender to be capable of rewriting all conceivable network protocols which are being transmitted from different devices.

An analogous adaptive technique is Active OS Fingerprinting, in which one or more packets are transmitted to a device so as to activate a visible response [2]. Passive and Active Fingerprinting was formalised by Shu and Lee, who also devised the Parameterized Extended Finite State Machine (PEFSM) to model behaviour when numerous messages were transmitted and received [49]. Likewise, Greenwald and Thomas investigated Active Fingerprinting and demonstrated that information gain can be employed to reduce the number of probes that were required [16]. Kohno et al. employed passive observations of the TCP Timestamp option to fingerprint individual devices according to their clock skew [30]. Similarly Formby et al presented Cross-Layer Response Times to fingerprint devices passively on enterprise networks [13].

Although all the aforementioned techniques associated with Operating System Fingerprinting are beneficial, they are not adaptive and can be disruptive to a network workflows. However, a new technique, entitled ”OS Fingerprinting Multi-Session Model Based on TCP/IP, HTTP and TLS” developed by Anderson and McGrew [2], appear to have addressed the shortcoming of the previous techniques. The OS Fingerprinting Multi-Session Model Based on TCP/IP, HTTP and TLS is a strictly ”passive” technique which is both adaptive and much less disruptive to networks and applications. Moreover, this technique is easier to be assimilated into network monitoring workflows and facilitates backward-looking discovery. These techniques employ data features from TLS in addition to TCP/IP and HTTP protocols in a multi-session model, which is pertinent whenever several sessions can be observed within a time window.

By employing TCP/IP, HTTP, and TLS features combined within the multi-session model, accurate fingerprinting is possible, even to the extent of minor version detection. A machine learning classifier is capable of addressing the multitude of data features efficiently providing more accuracy than single session fingerprints. The incorporation of TLS fingerprints for operating system identification is predominantly vital since the TLS-encrypted HTTPS protocol substituted for HTTP, and the traditional User-Agent strings will no longer be visible. The multi-session model enables cyber-defenders easily to include additional, explicit fingerprinting data types, which are important characteristics of an adaptive fingerprinting scheme. The multi-session model based on TLS, HTTP, and TCP/IP can detect vulnerable operating systems with higher accuracy, and that fingerprinting can be both adaptive and robust even when confronted with levels of data feature obfuscation that could be observed on an enterprise network.

4.6 Address Space Layout Randomization

Address Space Layout Randomization (ASLR) is often carried out offline at application code compile time in order for a decision to utilise ASLR to be open-loop in the control sense. The ASLR techniques stop attackers from locating target functions by randomizing the process layout. Previous ASLR techniques protected only against single-target brute force attacks, which worked by locating a single, supreme system library function such as execve(). However, such techniques were not adequate to guard against chained return-into-lib(c) attacks that invoke a series of system library functions. Thus, the research community built upon this technique to address its shortcomings. For instance, Xu and Chapin proposed the Island Code Transformation (ICT) that addresses chained return-into-lib(c) attacks [65]. A code island is a chunk of code that is isolated in the address space from other code blocks. This code not only randomises the base pointers used in memory mapping but also maximizes the entropy in function layout. There are various other types of Adaptation Techniques, the descriptions of which are outside the scope of this paper due to the space constraint. These include, for instance:

- Bio-Inspired Defences.
- Randomized Instruction Set and Memory Layout,
- Randomized Compiling,
- Just-in-Time Compiling and Decryption,
- Dynamic Virtualization,
- Workload and Service Migration, and
- System Regeneration.

4.7 Discussion on the Existing Adaptation Techniques

From the survey and the analysis of the above discussed Adaptation Techniques (ATs), it can be deduced that there exist various potential trade-offs when considering fundamental assignment, the perceived attack type as well as the system adaptation methods present by means of AT methods. It can also be deduced that although there are various ATs, the settings in which they are valuable to the defenders can differ significantly. Often, the major focus of research on ATs has been on engineering particular new techniques in contrast with comprehending their overall functionality and costs, when they can be most beneficial, what their potential inter-relationship can be. Despite the fact that each AT is likely to have some design accuracy, the discipline is still based on ad hoc approaches in relation to comprehending the entirety of ATs and their augmented use.

5 Human Factors and Psychology of Attack

One of the main factors that should be considered when developing a security policy within a firm is the contemplation of human factors and the psychology of cyber-attacks. The existing research on the social and psychological factors of cyber-attacks are conducted mostly by computer security and forensics specialists rather than by the social scientists [37]. Some of the reasons and motivations behind cyber-attacks are commonly listed in numerous sources as financial motivations, enjoyment and personal fun, political reasons also known as 'Hacktivism' [34], disruption, etc. Nevertheless, considering the behaviour and psychology of cybercriminals would not be sufficient. Gaining an understanding of the behavioural requirements of the victims is also necessary.

Nudge theory first introduced by James Wilk [63] discusses how small suggestions could influence the decision making of an individual or a group in favour of the proposer's intentions. Such theoretical underpinning could be potentially used by the adversary to gain positive compliance of a victim e.g. in a social engineering scenario.

Another psychological and behavioural notion that could assist cybercriminologists is the COM-B System [38]. Within this framework, motivation is influenced by capability and opportunity. Opportunity, capability and motivation are all influenced by behaviour. Understanding the causality within of elements within the cyber-crimiology context will pave the way to develop a holistic cyber security policy which would ultimately assist businesses to be able to defend against potential cybercrimes.

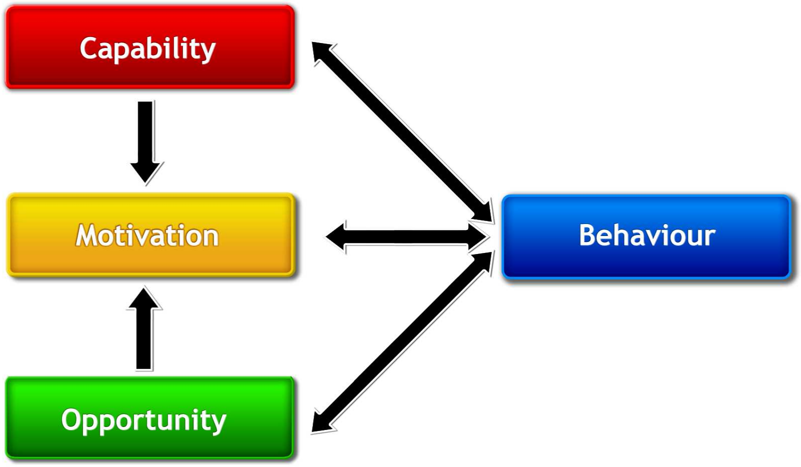

Fig. 2 COM-B behavioral Model [38]

6 Conclusions

Cyber-attackers are constantly devising new and sophisticated attacks, while traditional cyber-security approaches can only deal with known attacks and might prevent those attacks only temporarily and partially. Thus, new scientific foundation and the corresponding technologies are required in order to deal effectively with adaptive and dynamic cyber operations given that adversaries are increasingly becoming sophisticated. The efficiency of any cyber-defence system adaptation technology are unlikely to be quantified in a laborious way without such a scientific foundation.

Furthermore, there can be a significant improvement in security and a more effective cyber defence by employing established security policies and strategies such as those discussed in this paper. The use of such a solution provides an opportunity for the cyber defenders to have a new set of tools for both network and cyber environments that are established to be beneficial to enterprises. The policies and strategies discussed in this paper will enable enterprises to have a more robust security posture. Implementing these steps will ensure that the principles of carrying out operation are valued. This can be materialized, firstly, by ensuring that the enterprises possess a robust governance model that will encourage participation and compliance from both employees and managers. The cooperation between the members of the leadership team in relation to a common approach and set of objectives will help to consolidate the role and standing of cyber governance panel boards. Secondly, the distribution of intelligence both internally and externally will enable boosting the enterprises network and cyber security stance and reducing the response time of the cyber defenders. Thirdly, having an appropriate ratio of cyber defenders to the employees as suggested by [15] is essential to provide and uphold a sense of security and to benefit from the collected intelligence. Lastly, by adopting complexity theorys principles of systems analysis, the cyber defenders will be able to focus on protecting the points between systems that are vital to survival with higher effectiveness and with less trial and error.

Finally, to mitigate the limitations associated with traditional cyber-defence systems, it is imperative to design and implement new adaptive network and cyber security systems to combat attacks in these domains more effectively, such as those described in this paper. Such adaptive security systems based on intelligent Adaptive Techniques (such as those described in this paper) can also help to fuse information from various sources more effectively and also to profile cyber attackers more efficiently.

References

1. Aagedal, J.O., Den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D. and Stolen, K. (2002). Model-Based Risk Assessment to Improve Enterprise Security. The 6th International Conference on Enterprise Distributed Object Computing, pp. 51-62.
2. Anderson, B. and McGrew, D. (2017). OS Fingerprinting: New Techniques and a Study of Information Gain and Obfuscation, Cisco Systems, Inc. arXiv preprint arXiv: 1706.08003.
3. Apostolaki, M., Zohar, A. and Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. IEEE Symposium on Security and Privacy (SP), pp. 375-392.
4. Bada, M., Creese, S., Goldsmith, M., Mitchell, C. and Phillips, E. (2014). Computer Security Incident Response Teams (CSIRTs) An Overview. Global Cyber Security Capacity Centre, pp.1-23.
5. Chen, B., Peng, X., Yu, Y., Nuseibeh, B. and Zhao, W. (2014). Self-Adaptation through Incremental Generative Model Transformations at Runtime. The 36th International Conference

on Software Engineering, pp. 676-687.

6. Cheswick, W.R., Bellovin, S.M. and Rubin, A.D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Longman Publishing, 2nd edition.
7. Cybenko, G., Jajodia, S., Wellman, M.P. and Liu, P. (2014). Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundation. International Conference on Information Systems Security, pp. 1-8. Springer, Cham.
8. DeBruhl, B. and Tague, P. (2014). Keeping up with the Jammers: Observe-and-Adapt Algorithms for Studying Mutually Adaptive Opponents. Pervasive and Mobile Computing, 12, pp.244-257.
9. De Castro, L.N. and Timmis, J. (2002). Artificial Immune Systems: A New Computational Intelligence Approach. Springer Science & Business Media.
10. Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J.A. and Paxson, V. (2017). The Security Impact of HTTPS Interception. Symposium (NDSS′17) on Network and Distributed Systems, pp.1-14.
11. Elkhodary, A. and Whittle, J. (2007). A Survey of Approaches to Adaptive Application Security. International Workshop on Software Engineering for Adaptive and Self-Managing Systems, p. 16.
12. ENISA, Symantec Inc., Landitd Ltd. (2009). Good Practice Guide Network Security Information Exchanges. Special Publication (ENISA) - Rev 1.
13. Formby, D., Srinivasan, P., Leonard, A., Rogers, J. and Beyah, R. A. (2016). Who′s in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems. NDSS.
14. Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C., Querterman, J. and Scheier, B. (2003). CyberInsecurity: The Cost of Monopoly-How the Dominance of Microsoft′s Products Poses a Risk to Security. Computer and Communications Industry Association.
15. Godin, A. (2017). Using COIN Doctrine to Improve Cyber Security Policies. Available at: https://www.sans.org/reading-room/whitepapers/policyissues/coin-doctrine-improve-cyber-security-policies-37557 (Accessed: 26th August 2017).
16. Greenwald, L.G. and Thomas, T.J. (2007). Toward Undetected Operating System Fingerprinting. USENIX Workshop on Offensive Technologies (WOOT), pp.1-10.
17. HackerWarehouse (2017). MiniPwner Penetration Testing Toolbox. Available at: http://hackerwarehouse.com/product/minipwner/ (Accessed: 28th August 2017).
18. Haley, C., Laney, R., Moffett, J. and Nuseibeh, B. (2008). Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Transactions on Software Engineering, 34 (1), pp.133-153.
19. Hosseinpournajarkolaei, A., Jahankhani, H. and Hosseinian-Far, A. (2014) Vulnerability considerations for power line communication?s supervisory control and data acquisition. International Journal of Electronic Security and Digital Forensics, Inderscience, 6(2), pp. 104-114.
20. Husk, M., Cermk, M., Jirsk, T. and Celeda, P. (2015). Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. International Conference on Availability, Reliability and Security (ARES), 2015 10th, pp. 389-396.
21. Jahankhani, H., Al-Nemrat, A. and Hosseinian-Far, A. (2014) Cyber crime Classification and Characteristics. Cyber Crime and Cyber Terrorism Investigator′s Handbook. Vol. 1. Elsevier, pp.149-164.
22. Jahankhani, H. and Hosseinian-Far, A. (2017) Challenges of Cloud Forensics. Enterprise Security, Springer, pp. 1-18.
23. Jahankhani, H. and Hosseinian-Far, A. (2014) Digital Forensics Education, Training, and Awareness. Cyber Crime and Cyber Terrorism Investigator′s Handbook. Vol. 1. Elsevier, pp. 91-100.
24. Jajodia, S., Ghosh, A.K., Subrahmanian, V.S., Swarup, V., Wang, C. and Wang, X.S. (2012, a). Moving Target Defense II: Application of Game Theory and Adversarial Modeling. Vol. 100. Springer Science & Business Media.
25. Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C. and Wang, X.S. (2011, b). Moving target defense: Creating Asymmetric Uncertainty for Cyber Threats, Vol. 54. Springer Science & Business Media.

26. Janssen, M. and Kuk, G. (2006). A Complex Adaptive System Perspective of Enterprise Architecture in Electronic Government. The 39th Annual Hawaii International Conference on System Sciences, (4), pp. 71b-71b.
27. Jones, M.T. (2015). Artificial Intelligence: A Systems Approach: A Systems Approach. Jones & Bartlett Learning.
28. Kaspersky Lab. (2016). Kaspersky Security Solutions for Enterprise: Securing the Enterprise. Available at:
http://media.kaspersky.com/pdf/b2b/ (Accessed: 15th August 2017).
29. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015). A Survey of Cyber Security Management in Industrial Control Systems. International Journal of Critical Infrastructure Protection, pp.52-80.
30. Kohno, T., Broido, A. and Claffy, K.C. (2005). Remote Physical Device Fingerprinting. IEEE Transactions on Dependable and Secure Computing, 2(2), pp.93-108.
31. Lamsweerde, A.V. (2004). Elaborating Security Requirements by Construction of Intentional Anti-Models. 26th International Conference on Software Engineering, pp. 148-157.
32. Lei, C., Zhang, H.Q., Ma, D.H. and Yang, Y.J. (2017). Network Moving Target Defense Technique Based on Self-Adaptive End-Point Hopping. Arabian Journal for Science and Engineering, pp.1-14.
33. Lippmann, R., Fried, D., Piwowarski, K. and Streilein, W. (2003). Passive Operating System Identification from TCP/IP Packet Headers. IEEE Workshop on Data Mining for Computer Security, p. 40-49.
34. Ludlow, P. (2013). What Is a ?Hacktivist?? NYTimes. Available at:
https://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/
35. MacDonald, N. and Firstbrook, P. (2014). Designing an Adaptive Security Architecture for Protection from Advanced Attacks. Available at:
https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection (Accessed: 14th August 2017).
36. Markmann, C., Darkow, I.L. and von der Gracht, H. (2013). A Delphi-Based Risk Analysis?Identifying and Assessing Future Challenges for Supply Chain Security in a Multi-Stakeholder Environment. Technological Forecasting and Social Change, 80(9), pp.1815-1833.
37. McAlaney, J., Thackray, H. and Taylor, A., (2016). The social psychology of cybersecurity. The British Psychological Society, 29, pp. 686-689.
38. Michie, S., van Stralen, M. M. and West, R., (2003). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Science, 6(42).
39. Moffett, J. and Nuseibeh, A., (2003). A Framework for Security Requirements Engineering. Report-University of York Department of Computer Science YCS, pp. 1-30.
40. Mowery, K., Bogenreif, D., Yilek, S. and Shacham, H. (2011). Fingerprinting Information in JavaScript Implementations. Proceedings of W2SP, pp.180-193.
41. Nagurney, A., Daniele, P. and Shukla, S. (2017). A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints. Annals of Operations Research, 248(1-2), pp.405-427, IGI Global.
42. NCSC. (2017). The National Cyber Security Centre: a Part of GCHQ. Available at:
https://www.ncsc.gov.uk/ (Accessed: 28th August 2017).
43. Nhlabatsi, A., Nuseibeh, B. and Yu, Y. (2012). Security Requirements Engineering for Evolving Software Systems: A Survey. Security-Aware Systems Applications and Software Development Methods, pp. 108-128.
44. PA Consulting Group (PACG) (2015). Security for Industrial Control Systems - Improve Awareness and Skills: A Good Practice Guide. PACG special publication.
45. PA Consulting Group (PACG). (2015). Security for Industrial Control Systems: Improve Awareness and Skills - A good Practice Guide. Special Publication (CPNI) Rev 1.
46. Pasquale, L., Ghezzi, C., Menghi, C., Tsigkanos, C. and Nuseibeh, B. (2014). Topology aware adaptive security. The 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, pp. 43-48.

47. Peltier, T. (2016). Information Security Policies, Procedures, and Standards: Guidelines for effective Information Security Management. CRC Press.
48. Salehie, M., Pasquale, L., Omoronyia, I., Ali, R. and Nuseibeh, B. (2012). Requirements-Driven Adaptive Security: Protecting Variable Assets at Runtime. 20th IEEE International Conference on Requirements Engineering, pp.111-120.
49. Shu, G. and Lee, D. (2006). Network Protocol System Fingerprinting - A Formal Approach. 25th IEEE International Conference on Computer Communications, pp. 1-12.
50. Spitzner, I. (2008). Know Your Enemy: Passive Fingerprinting. Available at: https://www.honeynet.org/papers/finger (Accessed: 23rd August 2017).
51. Stoneburner, G., Goguen, A. and Feringa, A. (2002). Risk Management Guide for Information Technology Systems and Underlying Technical Models for Information Technology Security. Pennsylvania: Diane Publishing Company.
52. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. Special Publication (NIST SP)-800-82 Rev 2.
53. Sun, K. and Jajodia, S. (2014). Protecting Enterprise Networks through Attack Surface Expansion. ACM Workshop on Cyber Security Analytics, Intelligence and Automation, pp. 29-32.
54. Symantec Inc. and Landitd Ltd, (2009). Good Practice Guide Network Security Information Exchanges.
55. Tague, P. (2017). Inference-Based Adaptation Techniques for Next Generation Jamming and Anti-Jamming Capabilities. Available at: https://www.cylab.cmu.edu/research/projects/2013/inference-based-adaptation-jamming.html (Accessed: 27th August 2017).
56. Tyagi, R., Paul, T., Manoj, B.S. and Thanudas, B. (2015). Packet Inspection for Unauthorized OS Detection in Enterprises. IEEE Security & Privacy, 13(4), pp.60-65.
57. US-CERT (2017). Information Sharing Specifications for Cybersecurity. Available at: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity? (Accessed: 24th August 2017).
58. Vectra. (2016). How Vectra Enables the Implementation of an Adaptive Security Architecture. Available at: https://info.vectranetworks.com/hubfs/how-vectra-enables-the-implementation-of-an-adaptive-security-architecture.pdf?t=1487862985000 (Accessed: 28th August 2017).
59. Virvilis, N. and Gritzalis, D. (2013). The Big Four-What We Did Wrong in Advanced Persistent Threat Detection. 8th International Conference on Availability, Reliability and Security (ARES), pp. 248-254).
60. Wang, L. and Wu, D. (2016). Moving Target Defense against Network Reconnaissance with Software Defined Networking. International Conference on Information Security, pp. 203-217.
61. Wei, W., Suh, K., Wang, B., Gu, Y., Kurose, J. and Towsley, D. (2007). Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs. 7th ACM SIGCOMM conference on Internet measurement, pp. 365-378.
62. Weise, J. (2008). Designing an Adaptive Security Architecture. Sun Global Systems Engineering Security Office, pp.1-18.
63. Wilk, J. (1999). Mind, Nature and Emerging Science of Change: An introduction to metamorphology. Metadebates on Science, 24, pp. 71-87.
64. Wilkinson, M. (2006). Designing an ′Adaptive′ Enterprise Architecture. BT Technology Journal, 24(4), pp. 81-92.
65. Xu, H. and Chapin, S.J. (2009). Address-Space Layout Randomization Using Code Islands. Journal of Computer Security, 17(3), pp. 331-362.
66. Zalewski, M. (2014, a). p0f - Passive OS Fingerprinting Tool. Available at: http://lcamtuf.coredump.cx/p0f3/ (Accessed: 16th August 2017).