Abstract

Security is without a doubt at the top of the list of disciplines that are struggling to achieve acceptance as a specialty. Despite the important part that private security plays in society, it is unquestionably regarded as a job, unlike other professions. Security science is currently being treated as an emerging profession founded on logic and an applied set of ideas, which have been tested and modified to strengthen security services in the contemporary society. The aim of this crucial research is to assess the importance of security science in the contemporary society, with an emphasis on the ever-changing security issues. To assess the historical context, evolution, and realistic application of security science in a technologically advanced society, a content analysis research design is used. The compilation of opinion pieces, journals, essays, and speeches by reputable private security bodies and staff serve as the study's foundation.

Preliminary literature reviewed reveals that security science directs, informs, and quantifies the security mitigation strategies as it integrates security principles, the built environment, and security management in the contemporary society. Security principles constitute detecting, deterring, and responding to crises and risks while the built environment includes the physical and technical environment in which individuals play, work, and live. Security management, on the other hand, entails policy and procedures, awareness, and administrative roles. As a result, security practitioners and service providers should consider the function of security science in contemporary society and regard it as an evolving discipline and a profession of significance moving forward.

Keywords: Security principles, Built environment, and security management.

1. Introduction

Definition of security science

The word security is derived from the Latin word Securis, meaning freedom from anxiety. The freedom an individual has gained from potential harm from other people or objects in their environment is referred to as security. Food security, information security, home security, human security, national security, and corporate security are only a few examples of the various forms in which security can be provided. However, security science refers to a discipline that brings together most subjects in Security into one main structure characterized by knowledge.
According to studies by Smith & Brooks (2012), security science is defined as the discipline or idea that brings together other sub-disciplines with different concepts and subjects into a developing and structured entity of knowledge. These concepts and subjects can turn into theories in the future.

The concept of security is diverse, thus complicating its definition. Unlike other disciplines with an inclusive definition, security is understood in individual, national and international concerns. Brooks (2010) notes that the term “security” is widely used, and its scope has not changed to take into account a broader range of meanings. Security advances have inspired many literary imaginations and current studies with new findings. Such studies highlight the importance of taking into account the changing paradigms of security in the twenty-first century.

Science employs a series of procedures to demonstrate how results are arrived at. Security science, therefore, adopts a process of inquiry to test and criticize outcomes for improving both homeland and organizational security. A basic approach of security science entails gathering data, constructing an idea, evaluating the idea, and analyzing the outcomes of the experiment. This is important because security is both preventative and reactive for incidents that endanger human life and property.

In today's culture, security is viewed in a variety of ways. Cybersecurity, human security, cooperative security, and global security are all synonyms for the general word security used in economic and political discourse. Notably, security is multidimensional not only in principle but also in practice. As a result, it is essential to comprehend it in context. Fischer et al. (2008) argues that security is a state of stability, enabling people to pursue their activities without harm, disruption, or fear of injury. However, Post and Kingsbury (1991) adopt a more traditional definition of security as a service concerned with protecting the community, individual safety, and protection of assets and information. Another factor considered when defining security is its nature, whether private or public. Private security entails providing paid services to prevent, respond to and mitigate losses to property and safeguard people's lives.

Security in the twenty-first century may be objective, subjective, or symbolic. Private security's objectivity includes securing doors or the use of locks and keys. Subjectivity, on the other hand, includes practices such as CCTV installation in public and meeting areas. In the aviation sector, symbolic security is taking preventive measures such as restricting travelers from carrying too much liquid.

This research also presents ideas that characterize security science. According to the security science theory, there are no features that characterize the security discipline (Brooks, 2010). Instead, the theory incorporates a number of elements that can be used to describe security, including the objective, subjective, and symbolic essence of security. The theoretical definition of security science also includes a formula that entails various components. These components include an asset, which is denoted by letter A, and a level of protection which is offered by an individual or a group denoted by P. The asset has to encounter some level of threat which is denoted by letter T. Further, these variables, when brought together, have to adhere to a particular environment or situation denoted by letter S (Smith & Brooks, 2012). These concepts, therefore, provide the different elements of security science.
2. HISTORY OF SECURITY SCIENCE

Security development and growth have a distinct historical discourse as, since the beginning of time, man has sought and found ways of protecting himself and his properties. Guards were once hired by kings and noble families to protect them and their precious possessions. Their gold and silver were held in safes that were tightly sealed and secured. The concept of security, therefore, is not a recent phenomenon, even though the way in which it is applied has evolved. When World War I ended in 1918, it left a trail of widespread death and hate among citizens and nations. As nations grappled with the problem of security and keeping safe, security solutions were presented. World War I catalyzed the security profession. Since 1918, International security studies have increasingly expanded in several fields, as people seek better ways to protect themselves and what they own (Gill, 2014).

At certain points, new security inventions could promote security even with the reduction or absence of physical guards. For instance, in 1989, CCTV surveillance cameras were introduced after the publication of the famous George Orwell novel (Smith & Brooks, 2012). Security has progressed significantly over the years. This is attributed to the expansion of international relations, as well as technological advancements.

Before 1945, the consequences of World War I and the resulting insecurity were felt all over the world. Countries grappled with the reality of massive loss of life and incredible property damage. The introduction of technologies and guns used during the war added to the reason for alarm. This opened gates for environmental insecurity and breeding grounds for terrorism activities, and later the cold war (Gill, 2014). The Cold War meant looking for a better solution to avert another major war, which would cause more insecurity. International relations emphasized peaceful coexistence among countries as the key to fostering global security. Many other ideas, including Kenneth Waltz's popular Theory of International Relations, have aided cooperation on security issues.

International security studies have moved from superpower rivalry and nuclear weapons to diversified disciplines, which include, human, economic, and military security. In contemporary times, the risks of insecurity are not as insurmountable as they were in the early years when there were no sufficient security studies among the population (Smith & Brooks, 2012). With the introduction of foreign relations, security policies in all facets of life, from the world to the citizens, have improved. Safety experts and think tanks adhere to a set of protocols and standards in order to maintain and facilitate security, respond to security threats, and even anticipate potential security threats. This is achieved by the application of rapidly emerging technologies (Gill, 2014).

With the help of political scientists and economists Thomas Schelling and Henry Kissinger, whose primary focus was on nuclear deterrence, security studies have greatly developed to many and diversified fields like critical security studies, feminist security studies, public policy, and even criminology (Gill, 2014). Much has been learned about human rights, consultants, emergency management, intelligence, foreign policy, and dispute resolution in the context of international relations.
3. EVOLUTION OF SECURITY SCIENCE

Evolution reveals the reasoning shift without presuming a certain result or making any predictions. It charts the successes but also the failures and extinctions. International Security establishes a system of five guiding forces to define the major environmental pressures and how it adapts to them. Due to war and armed conflicts that have seriously affected the daily living conditions of various people throughout history, international security was started as a way of reducing the threats and consequences of different misunderstandings, to improve their coexistence on earth (William, 2010). Internationally, private security is required to protect from criminal gangs, terrorism, epidemics, dangerous foods, poverty, and destructions of nature, among many global difficulties. The safety of a nation and its citizens is much more critical than their misery.

Security enhances the protection and safety of a country's population. Their top priority must be tackled. The first scholarly history of international security examines how superpower competition and nuclear weapons have influenced environmental, economic, human, and other security concerns, in addition to military security, ranging from traditional research to feminism and post-colonialism. Its abilities have been used to force, strengthen, and provide authority in a variety of debates. Following the end of the Cold War in 1945, protection, rather than defense or war, became a guiding philosophy, raising political questions such as the importance of social stability in the relationship between military and non-military threats and vulnerabilities. It sought to catch the concept of grappling with defense, war, and conflicts, as well as the ambiguity of the word as a symbol. Although security has different meanings, rhetorical and political powers involved in security are emphasized in laying out the capacity of security or the policy to subordinate all other interests to those of the country. The Cold War and nuclear missiles were debated, as there were several conflicting guidelines on how to deploy, use, and not use military means during the nuclear period. The unusual strategic dynamics provided by nuclear weapons during WWII were linked to both the United Kingdom's and the United States' Cold War mobilization during WWII (William, 2010). Strategic bombing and nuclear weapons go beyond conventional military warfighting experience in ways that necessitate bringing in civilian experts ranging from physicists and economists to sociologists and psychologists, at the very least. Not only did it necessitate knowledge of how to best disable the enemy's military forces, but it also necessitated knowledge of how to best disable the enemy's economy and infrastructure.

Security at large requires sober minds to achieve the common goal of attaining peace, order, and stability at all costs. The central concept is an understanding of the identity of the opposing enemy, what relationship between the American and western Self and the Communist could be; hence, how security should be pursued (Fischer et al. 2008). The historical approach aided in demonstrating how deeper systems were built to combat emerging security challenges and ways to challenge them to prevent re-emergence.
4. PRACTICAL APPLICATION OF SECURITY SCIENCE

Security science is a combination of several concepts and principles. The knowledge of the security science encompassed in its principles is to deter, delay, and recover criminal offender studies (Hinks et al. 2006). The practical applications of security science are diverse concepts. It is applied in diverse fields of study. It is a broad topic that covers software vulnerabilities in web applications and application programming interfaces, cloud security, cryptography, infrastructure security, incidence response, and vulnerability management. Another practical application of the security science is the use of security studies in information management to prevent data breaches by halting and retrieving data before it is lost.

According to Hinks et al. (2006), security is diverse, cross-disciplined, and without a defined or specific knowledge or skill structure. The principles of emerging security disciplines are applied in the areas of asset protection, government-related disciplines, and the commercial security industry. The interplay of practical applications relates to the traditional forms of security approaches in the context of national and international systems through a country's military and defense systems. The traditional types of functional security applications, such as inter-state and national security, are used in this sense in foreign states. National state security, in many instances, is the involvement of the police forces to act as security personnel in the provision of security to the citizens; a few examples are the defense systems in homeland security.

Traditional security elements may be classified as either public or private, depending on who is providing the security services. The use of police systems in the government allows the public aspect, while specialized staff licensed to own weapons for their personal and individual protection make up the private sector. According to Fischer et al. (2008), the new international security climate has seen the erosion of conventional states as a result of expanded globalisation and access to global intelligence and networks, which has also fused defense and security. The traditional definition of the security science is the physical aspect of security bodies. This guarantees that a country's autonomy is maintained in accordance with the governing principles and laws enshrined in its respective constitutions. The multi-dimensions of security science are quantified by the probability of a multi-discipline aspect of security.

The issue of protection can be exploited for political and intellectual gain. The idea of securitization is born as a result of this, and it can be applied to all military, environmental, economic, and social sectors. This, however, does not apply at the personal level. Securitization highlights the intellectual and political aspects of security in a wider range of issues. It gives meaning to security and confines its scope to a justifiable context when extended to an analytical and grounding context (Smith & Brooks, 2012). Security is an issue connected to the survival of an object from an existential threat. Without this, it becomes meaningless to be termed security. Securitization is achieved when an issue is treated as a security issue based on the stated parameters of being a threat and reasonably uses exceptional political measures to solve the breach. Fischer et al. (2008) demonstrated that securitization is a continuum that ranges from non-politicized to a national discussion and then counts as an existential challenge, justifying reactions that go beyond conventional political processes.

As technologies and information infrastructure progress, information from different sectors is at risk of being compromised and exposed to the public, as well as falling into the hands of unwanted individuals. Therefore, a method for mitigating the negative
consequences of technology had to be created. As a result, the concept of cybersecurity emerged (Fischer et al. 2008). The increased integration and diversification of administrative enterprises created a wider scope and exposed the information of the companies to threats. The data may not be safe and secure in such aspects as it is exposed to the internet, easily hacked, and decrypted by specialists. Cybersecurity in the operation of the metrication frameworks contains a metamodel over the Security to support the assessment. These security metamodels, conceptual models, and technical reference models can support cybersecurity assessments and be used in the processes where one needs to gauge the cybersecurity metrics.

The metrication methods describe how the variables are put together to generate a more detailed and meaningful result to help solve the problem of loss of data, exposure of data, and many other threats to securitization and security of data from an organisation or company. As Sommestad et al. (2010) explains, security is both a need and a philosophical idea. The matrix formats also demonstrate the extensions and domains that explain the scope of the regarded security problem in question.

The security studies from the perspective of criminal justice give a platform and an organogram of laws and legal suites that help solve the problems brought about by the breach and interference of an organisation's data (Fischer et al. 2008). The law critically describes the context of Security of data from the point of inception to the storage, the limitations and prospects of personnel who are in a position to access the data, and the punishments or legal measures that come with the problem caused.

Cryptography is a security science application that aids in the storage and management of data to prevent it from falling into the hands of untrustworthy individuals. It helps in protecting information and communications through the use of codes and technical coding. The crypt is confidential information where the message can only be decrypted and read by the person for whom the message is strictly intended without falling into other people's hands (Sommestad et al., 2010). Even if the above knowledge reaches the hands of others, they will never be able to perceive and comprehend it in context. Hidden key, public key, and hash functions are well-established and widely used methods of security encryption with algorithms that protect information from falling into the hands of a third party.

Cloud security is a realistic application of security science as well. Cloud security refers to the protection of data stored online via cloud computing platforms using techniques such as firewalls, obfuscation, penetration testing, tokenization, and virtual private networks, all of which are commonly used by participants in this technological era (Fink, 2006). The aforementioned cloud security contributes significantly to the privacy and security of data and information intended for storage (Fink, 2006). As a result, the data is secure from hacking, leakage, and deletion. The measures justify user and system authentication and control, as well as data privacy and resource validity protection.

Data protection and privacy are the first implementations of these security modes in the technical period. Data protection through cloud security is critical and has numerous applications in data privacy. Since the data can be processed according to the needs of the parties concerned, there is flexibility. There is also the issue of preventing the spread of denial-of-service attacks, which are becoming more common. The best cloud protection focuses on preventing massive traffic to avoid a data backlog, but devices can surge and break down in the process. As a result, cloud protection adoption is an important and realistic security implementation. It has greatly aided in the protection of records, the storage of larger data, and the integrity and privacy of the data stored. In the cryptography method, a firewall provides a temporary bridge that protects data from attack and loss. As technology advances,
individuals are constantly attempting to access, corrupt, and interact with data and knowledge.

The realistic applications are designed to address the highly motivated attackers' intent to bypass mitigation strategies by leveraging their expertise and resources (Fischer et al. 2008). In several cases of security, the mail service attack is the most widely known security breach. Malicious actors use mail service attacks to fuel and spread information across the internet.

5. CONCLUSION

In this technological age, security science has consistently assisted in addressing the flaws that have arisen as a result of the growth and rising rates of technology (Fischer et al. 2008). It has prevented communications from being intercepted and reaching unexpected recipients, especially when it comes to military officers' communications via short-wave radio. When a particular organisation is at risk of losing data and has to shield information from being intercepted, encryption guarantees the information's security. Cloud encryption also allows for greater data storage. As a result, there is no doubt that security science is relevant because it helps to overcome some of the security problems that come with technological innovation and living in a modern world.

6. REFERENCES