Birkbeck
UNIVERSITY OF LONDON

BIROn - Birkbeck Institutional Research Online

Trim, Peter and Lee, Y.-I. (2023) Combining sociocultural intelligence with Artificial Intelligence to increase organizational cyber security provision through enhanced resilience. In: Trim, Peter and Lee, Y.-I. (eds.) Managing Cybersecurity Threats and Increasing Organizational Resilience. Basel, Switzerland: MDPI, pp. 203-222. ISBN 9783036596440.

Downloaded from: https://eprints.bbk.ac.uk/id/eprint/52659/

Usage Guidelines:
Please refer to usage guidelines at https://eprints.bbk.ac.uk/policies.html or alternatively contact lib-eprints@bbk.ac.uk.

big data and cognitive computing

MDPI

Article

Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience

Peter R. J. Trim [1,*] and Yang-Im Lee [2]

[1] Department of Management, School of Business, Economics and Informatics, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK
[2] Department of Marketing and Business Strategy, Westminster Business School, University of Westminster, 35 Marylebone Road, London NW1 5LS, UK
* Correspondence: p.trim@bbk.ac.uk

Abstract: Although artificial intelligence (AI) and machine learning (ML) can be deployed to improve cyber security management, not all managers understand the different types of AI/ML and how they are to be deployed alongside the benefits associated with sociocultural intelligence. The aim of this paper was to provide a context within which managers can better appreciate the role that sociocultural intelligence plays so that they can better utilize AI/ML to facilitate cyber threat intelligence (CTI). We focused our attention on explaining how different approaches to intelligence (i.e., the intelligence cycle (IC) and the critical thinking process (CTP)) can be combined and linked with cyber threat intelligence (CTI) so that AI/ML is used effectively. A small group interview was undertaken with five senior security managers based in a range of companies, all of whom had extensive security knowledge and industry experience. The findings suggest that organizational learning, transformational leadership, organizational restructuring, crisis management, and corporate intelligence are fundamental components of threat intelligence and provide a basis upon which a cyber threat intelligence cycle process (CTICP) can be developed to aid the resilience building process. The benefit of this is to increase organizational resilience by more firmly integrating the intelligence activities of the business so that a proactive approach to cyber security management is achieved.

Keywords: artificial intelligence; cyber security manager; cyber threat intelligence; learning; resilience; sociocultural intelligence

check for updates

Citation: Trim, P.R.J.; Lee, Y.-I. Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience. *Big Data Cogn. Comput.* **2022**, *6*, 110. https://doi.org/10.3390/bdcc6040110

Academic Editor: Fabrizio Baiardi

Received: 26 August 2022
Accepted: 1 October 2022
Published: 8 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

For an organization to become more resilient, top management needs to take heed of the fact that cyber attacks are likely to intensify in the years ahead and because of this, cyber security needs to be placed in a strategic cyber security management context [1]. The need for such an approach is clear, bearing in mind that: "Even with U.S. company losses due to cyberattacks nearing a reported $1 trillion by late 2020, a survey of nearly 1000 organizations found that only 44% had cyber preparedness and incident response plans in place" [2] (p. 2). It seems logical, therefore, for managers to counteract cyber attacks by utilizing cyber security technology more fully, but also for them to discover new ways to engage in cyber security management. A key role of senior management is to help managers draw on operand and operant resources so that they can strengthen the organization's defenses against cyber attacks.

Advice relating to the appropriateness of cyber security technology comes in the form of government advice, highly specialized companies that operate cyber security technological solutions, consultants that have in-depth knowledge of cyber security problems and working practices, and university research teams that develop specific types of security software. There are, of course, other sources of intelligence that originate from government

agencies and specialist consultancies, for example. Taking this into account, it can be suggested that managers need to adopt a pro-active approach to cyber security as resilience requires that intelligence-gathering involves the deployment of technology that has the power of human cognition and the ability to learn/reason and hear/see [3] (p. 109). An important point that surfaces, however, is that to be effective, organizational resilience needs to be placed within the context of how organizational staff coordinate investment in cyber security across the supply chain [4] (p. 169). Bearing this in mind, it is pertinent to suggest that cyber security management is to be viewed as a strategic-level capability [5], whereby security is linked with business continuity management and a set of procedures whereby security is placed within a crisis/disaster management setting. The case can be made, therefore, for a cyber security manager to be appointed to take charge of cyber security, which is at the heart of an organization's security [1].

Understanding the motivations of those who carry out a cyber attack means having an in-depth appreciation of human behavior and establishing what causes an individual to behave in an anti-social/illegal manner. The cyber security manager is, therefore, required to have an appreciation of human psychology and possess adequate knowledge of how cyber security policy is formulated and implemented, if they are to provide guidance and advice to a range of functional heads. If a data breach does occur and results in reputational damage and an increase in adverse publicity resulting from a fine imposed by regulators, then cascading effects may have a debilitating effect on the organization and its trading partners. It is for this reason that the cyber security manager needs to have both technical and managerial knowledge relating to cyber security or have expertise available to them that can be drawn on when necessary.

The remit of the cyber security manager is to work with other senior managers and devise, manage, and implement cyber security policy decisions across the organization's networks. The focus of the research is, therefore, to explain how different approaches to intelligence (i.e., the intelligence cycle and the critical thinking process) can be combined and linked with cyber threat intelligence (CTI), which utilizes AI. To explain this, we explore how the cyber security manager can draw on social interaction and establish how it drives cognition [6] (p. 306). This can be viewed as logical in terms of establishing organizational resilience because cyber security management requires the cyber security manager to develop and share cyber security knowledge with individuals that are viewed as first responders. Social interaction is enhanced through trust-based relationships and open communication between staff and provides the basis for institutionalized learning. This gives rise to a defined risk mitigation policy and strategy within partner organizations and the utilization of cyber security models [7].

In terms of AI-based cyber attacks, it can be argued that cyber security experts will be required to intensify their effort to develop AI defense systems [8]. This will require that risk mitigation strategies are put in place to counteract cyber attacks; it also will focus attention on cyber defense from an intellectually driven and holistic perspective. It is with this in mind that the focus of the paper was to outline how sociocultural intelligence can be combined with AI to increase the organizational cyber security provision and enhance an organization's level of resilience. In doing so, we focused our efforts on providing answers to two questions: (1) How can a non-security specialist develop their appreciation and understanding of resilience through undertaking threat intelligence? (2) How can knowledge regarding different types of AI help managers better understand the complexities associated with different algorithms and their functionality vis-à-vis different types of defense system?

To assist us in our task, we drew on the knowledge derived from a small group interview that involved an academic researcher discussing various aspects of intelligence in relation to organizational security with five experts. Each participant had spent over twenty years in security and had worked in different industries and was known to be an expert in the field of organizational resilience. We contribute to the field of cyber security management by combining elements of the intelligence cycle (IC) with the critical thinking

process (CTP) [9] (p. 139) to produce a cyber threat intelligence cycle process (CTICP). This should enable staff to adopt a strategic cyber security intelligence perspective. We also highlight the importance of organizational learning and how it facilitates a higher level of intelligence that involves sociocultural interaction and thus makes the organization more resilient. The advantage of this approach is that we reflect on the interplay between centralized versus localized learning and how sociocultural intelligence is viewed as a necessary component of the strategic cyber security management process. Finally, through linking AI with sociocultural intelligence, we outline the steps in the cyber threat intelligence cycle process (CTICP) that enable managers across various industries to adopt a resilience centric approach that hardens the organization.

2. Background

Bearing in mind that those carrying out cyber attacks are becoming more sophisticated and linked more firmly to those carrying out all types of scams, the cyber security manager needs to make a value judgement with regard to how cyber threat intelligence (CTI) is perceived by top management and how, because operant resources are scarce, staff can draw on technological aids such as artificial intelligence (AI) to enhance their cyber threat intelligence (CTI) decision-making capability. Hasan et al. [10] (p. 354) indicated that the advanced persistent threat (APT) is challenging organizational defenses because signature-based defense mechanisms are unable to respond in real-time to new types of malicious code/intelligent mutant codes. It is worth noting that "Conventional cybersecurity tools look for historical matches to known malicious code, so hackers only have to modify small portions of that code to circumvent the defense. AI-enabled tools, on the other hand, can be trained to detect anomalies in broader patterns of network activity, thus presenting a more comprehensive and dynamic barrier to attack" [10] (p. 354).

Surya [11] (p. 991) has provided a useful definition of AI: "Artificial intelligence (AI) refers to the technology involved in the development of smart machines and software. This includes the developments of applications and systems that can reason, collect intelligence, prepare intelligently, learn, interact, interpret, and manipulate objects". Hence, AI allows users of big data to capture data from a variety of sources, store the data, and apply analytics so that decision-makers can use the outcome [11] (p. 992) in a variety of contexts (e.g., tactical and strategic).

AI can help managers to interpret patterns of cyber attack, and the outcome of a cyber threat intelligence (CTI) analysis can be placed in report form so that senior managers can offer advice based on the type of threat identified with a view to utilizing operand and operant resources. In addition, those charged with managing security can interact more fully with other functional managers and establish how cyber threat intelligence (CTI) can be strengthened using AI. However, it is worth noting that although it is recognized that AI can be used to defend an organization against cyber attacks [12] (p. 363), there are a number of challenges that senior management need to overcome vis-à-vis the use of AI. One such problem is the gap in knowledge relating to what AI/ML represents and how AI/ML can be used by managers operating at different levels of authority. It is possible to suggest that the complexities associated with AI/ML may well militate against individual managers understanding how AI can be used. To overcome the likely resistance of using AI, we propose that managers first develop an appreciation of AI/ML and think of how AI/ML can benefit them in terms of their decision-making so that the day-to-day operations are reinforced through contingency plans.

Managers need to be mindful of the fact that AI is refined through the application of ML but "humans are able to understand the behavior of others in terms of their mental states-intentions, beliefs and desires-by exploiting what is commonly designated as 'folk psychology'" [13] (p. 279). By acknowledging this, managers can avoid the various pitfalls associated with the use of AI, especially the contradiction whereby chatbots are used to help individuals (i.e., those using an organization's website) to gain certain information by responding/acting in known and logical ways. Gallese [13] (p. 285) suggests that although

it is possible to make sense of how people respond to an event, with regard to human social cognition, "Language is the most specific hallmark of what it means to be human". It is with this in mind that we reflect on and pose the question: how can sociocultural intelligence be linked with AI to increase an organization's resilience?

Before progressing, we consider it necessary to reflect on the notion of what resilience is and to have a clear understanding of what it incorporates. HSSAI [14] (p. 9) provides a useful definition of resilience by indicating that it is "the ability of a system to attain the objectives of resisting, absorbing, and recovering from the impact of an adverse event, before, during, and after its occurrence. It is also a dynamic process that seeks to learn from incidents to strengthen capabilities of the system in meeting future challenges. The goals are to maintain continuity of function, degrading gracefully, and recover system functionality to a pre-designated level, as rapidly as desired and feasible".

The focus is clearly to learn from an event/incident and to make sure that those with operational responsibility can "learn from incidents", as this is what machine learning sets out to achieve. In the context of organizational learning, whereby the focus of attention is on how an individual's skill level is enhanced, Argyris [15] (p. 8) provides guidance by indicating that: "Learning is defined as occurring under two conditions. First, learning occurs when an organization achieves what it intended; that is, there is a match between its design for action and the actuality or outcome. Second, learning occurs when a mismatch between intentions and outcomes is identified and it is corrected; that is, a mismatch it turned into a match".

Whether data are collected, analyzed, and interpreted by humans or are left to a machine(s) is not what is under consideration. What is important to acknowledge is that adequate resilience requires managers to consider how best to utilize intelligence and to make use of limited intelligence. McCreight [16] (p. 5) has offered a comprehensive view as to what resilience encompasses by indicating that there are five main dimensions of resilience, which are: personal and familial socio-psychological well-being; organizational and institutional restoration; economic and commercial resumption of services and productivity; restoring infrastructural systems integrity; and operational regularity of public safety and government. The five dimensions highlighted prove useful with regard to a manager developing a comprehensive understanding of what resilience involves and how to place resilience within an organization–government–society context. Whether the relationships developed are transactional in nature or transformational in nature depends upon the organization's value system, and the leadership style/model in place.

In order to utilize big data to counteract sophisticated cyber attacks, managers are paying increased attention to the capability of AI and its deployment. Hence, it is useful to acknowledge two main but contradictory issues: the volume of data that needs to be processed versus the time available to carry out an analysis, which yields an outcome that has relevance and can be acted upon. Additionally, attention needs to be given to the cost of hiring experts for labeling the data, which relates to the issue of supervised learning, semi-supervised learning, and unsupervised learning. In terms of cyber threat protection, deep learning (DL) is receiving renewed attention. For example, one area that needs immediate attention is ransomware attacks. Andrade and Yoo [17] (p. 2) noted that between 2014 and 2017, 327 families of ransomware were identified that accounted for 184 million attacks. Because cyber criminals are behind such attacks and do, of course, use technology to carry out their actions, it would be logical to suggest that advances in deep learning (DL) will help those involved in cyber security to protect computer systems and networks better. An interesting and relevant point raised by Andrade and Yoo [17] is how cyber security specialists can consider using psychology to enhance cyber security situation(al) awareness and they make clear that cognitive sciences can be utilized to enhance cyber security.

Bearing in mind that the focus of this paper was to deepen our understanding of cyber threat intelligence (CTI) and provide arguments as to how AI/ML can help senior managers to make an organization more resilient, we first need to take cognizance of what Dawson [18] (pp. 268–269) has said about an organization as it provides the basis for better

understanding the relational processes that allow individual managers to utilize technology for the benefit of the organization and its partners, and at the same time, provide the basis for strategic cyber security management [1] that is aimed at safeguarding the organization against cyber attack. Dawson [18] (pp. 268–269) highlights seven points that epitomize an organization: (i) an interactive system (e.g., change in one aspect will have repercussions for another); (ii) high level of complexity (e.g., uncertainty is evident); (iii) there is no single way in which to manage a situation; (iv) resources are scare; (v) different interest groups prevail (e.g., conflict, consensus and indifference are evident); (vi) constraints exist that effect action; and (vii) the level of the individual/group needs to be known in order to identify and solve problems. It is with these seven points in mind that we embrace the view that organizational resilience is dependent upon managers having a clear appreciation of what sociocultural intelligence involves and how AI can be utilized to enable managers to make more informed cyber security-based decisions.

3. Placing Sociocultural Intelligence in Perspective

The concept of sociocultural intelligence has been gaining momentum over a number of years and it is clear that the field of intelligence is expanding, and new perspectives are being offered that allow managers such as the cyber security manager to comprehend how intelligence is managed across organizational networks. To ensure that AI is not misused, we advocate a cautious and incremental approach to its use but also advise a wider understanding of AI's application in terms of intelligence provision. What can be deduced from the study of intelligence is that sociocultural intelligence (SOCINT) is purported to include "the process of directing, collecting data related to any of the social sciences, analyzing, producing, and then disseminating such data for situational awareness in any operational environment" [9] (p. 11). This is a well-known and accepted view. To better understand the antecedents of cyber threat intelligence CTI), we suggest that managers take cognizance of the intelligence cycle (IC) process and the critical thinking process (CTP), as outlined by Patton [9] (p. 139). The intelligence cycle (IC) is known to be composed of five separate but linked stages including (i) planning and direction; (ii) collection; (iii) processing; (iv) analysis and production; and (v) dissemination. The critical thinking process (CTP) is known to include eight separate but linked stages: (i) purpose; (ii) question at issue; (iii) information; (iv) interpretation and inference; (v) concepts; (vi) assumptions; (vii) implications and consequences; and (viii) point of view. By merging the intelligence cycle (IC) with the critical thinking process (CTP), it should be possible to establish how AI can be utilized by managers to better understand the role that cyber threat intelligence (CTI) plays and how it is to be managed across organizations. Before we explain this, we need to understand how the differences in learning capabilities associated with AI/ML can be drawn on to provide an intelligence focused appreciation, leading to an enhanced appreciation of resilience. To achieve this, we focused on AI/ML in relation to business so that managers in charge of various business functions can relate better to the learning capabilities afforded by AI/ML, and not worry too much about the technical aspects. Should managers need to, they can deepen their knowledge of AI/ML by consulting those with expert knowledge and/or attend specialist courses of study.

4. Algorithms and Their Learning Capability

Deep learning (DL) is a subset of AI, and it structures algorithms in layers to create an artificial neural network (e.g., a human brain) for filtering information and learning from it and making intelligent/informed decisions. DL applies ML to large datasets. ML uses algorithms to analyze, learn from the data, and make decisions based on the learning. Both DL and ML are subsets of AI. It is useful to note that different algorithms have their own unique functionality and capability for learning, some of which can be used for specific tasks. Table 1 shows different forms of learning in DL. AI systems can be divided into three types such as narrow AI (which is goal-oriented and programmed to perform a single task); general AI (representative of a machine that can learn, understand, and act in a way similar

to that of a human in a given situation); and super AI (a hypothetical AI where a machine exhibits intelligence that surpasses the brightest humans).

Table 1. The different types of learning associated with functionality/capability.

Functionality for Different Types of Learning	ML, DL, and AI Learning Style and Algorithm		Use of AI/ML in Business
Mechanical	ML—(un)supervised—minimum degree of learning		To predict similar event in future, e.g., utilize simple tasks such as greeting or simple order taking on behalf of waiters/waitresses; self-service. Algorithms for supervised learning such as: linear and logistic regression, decision tree, k-nearer neighborhood (KNN), naïve Bayes (NB), random Forest, neural network (NN), support vector machine (SVM). Algorithms for unsupervised learning such as: K-means clustering, factor analysis (FA), principal component analysis (PCA), DBSCAN, SVD.
Analytical	**DL—supervised**	**CNN**	Deep learning (DL) is inspired by the way a human brain works for filtering information, which helps a computer model to filter data through layers and classify information. Selecting an advertisement for a particular platform that will gain more popularity via surfing the Internet (to increase clickability based on algorithm learning to make a match between a particular advertisement that was placed and individuals that visit a particular site). Spam filter. DL network architectures are classified such as convolutional neural networks (CNN) and recurrent neural networks (RNN). Used widely for the use for visual image/object analysis, classification, e.g., search engines and recommender systems—Facebook/Google photos suggest tag by recognizing the face.
		RNN	It uses sequential data, which is distinguished by memory, and prior inputs influence current input and output, but the outcome can vary depending on the type of RNN such as for music generation, sentiment classification, and machine, e.g., IBM Watson Studio and Watson Machine Learning, trailers ("binging show") in Netflix, OTT platforms. Monitoring buying habits—particular types of platforms for shopping, surfing the purchasing history of groups of customers and placing them into similar purchasing segments to market specific items among suitable segments [19].
	DL—Semi-supervised learning (SSL)		Combination of supervised and unsupervised learning for data deduction and labeling from large unlabeled data. It can be used for graph-based label propagation; speech recognition; web content classification; text document classification (e.g., URL: https://www.altexsoft.com/blog/ (accessed on 15 June 2021)).
	DL—Unsupervised learning	Self-organizing maps Boltzmann Machines	Without human intervention, algorithms work on datasets to identify hidden patterns or for groupings based on similarities/differences in the data, e.g., useful for building recommend system (look at "rating" and "preference"). Typically, 2-dimentional representation. Useful for visualization. Handwritten and visual object recognition tasks [20].
Intuitive	AutoEncoders		Useful for reducing audio data, e.g., through anomaly detection algorithms to detect specific fraud.
Intuitive	**Reinforcement learning (RL)—ML/part of AI**		Watson's Jeopardy (question-and-answer system), AlphaGo, Mario, Deepmind, self-driven car, Keras (in libraries), etc. Alpha Zero (RL with AI).
Intuitive	Advanced AI—focused on cognition		Able to make a deductive decision based on the analysis of data and able to predict without data input like human (gut feeling based on cognition of patterns in the data).
Empathetic	Super Advanced AI—Focus on emotion and empathy		Identify consumer emotional status and interact empathetically through the use of natural language processing [21].

Source: The authors.

Managers in various industries such as banking, the motor industry, and health care have paid careful attention to AI implementation in relation to learning capabilities. Retailers utilize augmented reality for a better image (e.g., ASOS, visual search [22] and some retailers such as M&S and Kohl's have partnered with Snapchat and implemented a virtual fitting room [23]). The use of an avatar, a virtual character, with virtual reality and/or with a chatbot, is also gaining the attention of an increasing number of managers in business. It allows them to create virtual social touch points as well as create entertaining effects that result in a richer customer experience and higher customer engagement [24–26].

The application of methods and algorithms in AI/ML varies and produces a specific effect in the way in which the interaction process with end users is managed. Different algorithms also have implications for the types of data that are needed and how the data are captured and analyzed. AI is concerned with designing intelligent systems that exhibit characteristics associated with human intelligence and behavior and involves cognitive processes such as adapting to the latest information and problem-solving [27]. AI's capability varies, for example, Google Home and Alexa, integrate AI and advanced analytics (ML algorithms); chatbots sense the context of the conversation, but cannot perform a set of activities on their own; virtual assistants (e.g., Alexa, Apple Siri, Google assistant or Corona) provide daily activities such as emails or schedule meetings and can crawl through existing resources for a range of requests but with regard to customer service, however, they cannot resolve queries on their own [28] and friendly conversational chatbots such as Mitsuku and Replika, which are humanoid AI, are able to respond to emotional verbal reactions in a meaningful way [29,30]. What can be noted from this is that the communication process between a potential customer and the organization itself can be enriched by staff providing reassurance about the organization in terms of its resilience, which is mapped to an end user's understanding of security awareness. From this, we can identify the following question: how can an individual's learning capability be enhanced through using AI/ML? Finding an answer is important because managers need to link AI learning with the analysis of data and the interpretation of data so that the intelligence derived can be evidence based and used to underpin various plans/strategies. However, we stress that it is not just about AI enhancing what the organization is in terms of its commitment to dealing with customer requests or undertaking cyber threat intelligence (CTI) analysis. It is more about assuring external individuals that the staff are pro-active in terms of security awareness and can link the need for intelligence with the learning capability of those interested in buying the company's products and services, so they feel confident in buying from the company and avoid buying from rogue websites.

Learning can, according to Campbell et al. [31] and Ma and Sun [19] be divided into four types: supervised learning; semi-supervised learning; unsupervised learning; and reinforcement learning. In supervised learning, an expert trains the system by feeding labeled training data and defines variables to algorithms whereas in the case of unsupervised learning, the machine can learn inductively from unlabeled/unorganized data by analyzing the datasets to draw meaningful correlations or inferences by identifying hidden groups or grouping patterns. It can be noted that reinforcement learning (RL) is behavior-driven auto-learning where the algorithm/model (called agent) learns from interaction with its environment (by choosing from a set of possible actions) and their outcome. The sequential order and time plays an important role in reinforcement learning and is linked with a reward or penalty depending on the performance correctness and attempts to maximize the cumulative number of rewards.

The functions of AI/ML in an online business context can be grouped. For example, the basic mechanical function is an analytical tool, and the intuitive function includes humanoid AI [32]. Understanding different functions of AI/ML is useful as it helps managers to choose appropriate AI/ML tools in relation to the company's positioning strategy. We reiterate that the positioning strategy links learning with security awareness and is derived from the leadership style/model and organizational value system.

With regard to the basic mechanical function, it is based on rule-based learning at the minimum and relies on prior knowledge to perform repeated routines and/or transactional tasks (e.g., search engine used by Google or Bing). The analytical function relates to how information is processed for problem-solving in logical reasoning and how AI/ML tools learn from it. It is advanced, rule-based learning that carries out complex tasks and executes rational decisions (e.g., Deep Blue, IBM's chess player). The intuitive function incorporates digital technology that can mimic a human's learning intuitively. It is this, we feel, that can be used to ensure that sociocultural intelligence can be harnessed to get an individual to look more deeply at the issues relating to cyber threat intelligence (CTI) and map the outcomes to their own level of security awareness. Table 1 outlines the different types of AI/ML associated with learning and their use in business and is for illustrative purposes only. The differences in supervised learning, semi-supervised learning, unsupervised learning, and reinforcement learning are discussed next.

4.1. Supervised Learning

There are various algorithms for supervised learning such as a neural network (that has layers of nodes and trains data by mimicking the connectivity of the human brain, through each node being made up of inputs, weights, a threshold (bias)), and output; K-nearest neighbors (for prediction); naïve Bayes (is a classification method and well-used for text mining, spam filtering, and a recommend system); linear regression (used to identify relationships between a dependent and one or more independent variables); logistic regression (used to produce binary output by leveraging linear regression); support vector machine (SVM) (used for both data classification and regression, however, especially useful in the decision boundary to separate classes of data points); and decision tree (based on one input variable, each step split an existing subset into two, and has the capability of intuitive interpretations [19,33].

With respect to the analytical function of AI and ML, there are various levels of sophisticated applications [33,34]. For example, a convolutional neural network (CNN) is normally used for visual image analysis, classification, medial recreation, and is the recommended system, for example, whereas recurrent neural network (RNN) uses sequential data, which is distinguished by memory, and prior inputs influence the current input and output [19,35], but the outcome can vary depending on the type of RNN such as music generation, sentiment classification, and machine translation (e.g., IBM Watson Studio and Watson Machine Learning) [36]. The use of supervised learning in retail allows managers to use a shopper's basket datasheet to further define sub-segment groups by using the price of each product and the budget of an individual. It helps to uncover demand patterns for different products at different stores. For example, the combination of regression techniques may allow a retailer to predict the probability of a target variable (e.g., predict churn and switching behavior) that measures the satisfaction and engagement in the website characteristics and demographic information. This can be considered as confidence building from the perspective of the customer and provides them with a sense of well-being. However, supervised learning requires knowledge and the time to train the model, which can result in human error, which affects whether the algorithm performs as expected. Reflecting on this point, it can be suggested that should an error occur for whatever reason, it is likely that the end user will become less trusting of the technology and therefore seek to purchase another company's product/brand.

4.2. Semi-Supervised Learning (SSL)

The SSL approach is a combination of supervised and unsupervised ML. SSL uses small amounts of labeled data and a large amount of unlabeled data to train a model to label data. It is useful in a situation where limited labeled training data are available with a large amount of unlabeled samples [37]. According to Ouali et al. [38], SSL and its applications can be used to reduce the amount of labeled data required either by developing new methods or adopting existing SSL frameworks for a DL setting. For example, cluster

analysis is a method that groups datasets into homogenous subgroups that contain similar characteristics in the data such as the same gender or common group associations as the goal is to identify the similarities and differences between data points. The application of cluster analysis in SSL is to use some known cluster information to classify other unlabeled data, which uses both labeled and unlabeled data. There are various methods and approaches such as consistency regularization (or consistency training) for perturbed vision, for example, proxy-label uses a heuristic approach and leverages trained model on the labeled set to produce training examples by labeling unlabeled sets; generative models use learned features on one task that can be transferred to other tasks; and graph-based methods that propagate labels from labeled nodes to unlabeled nodes by using the similarities of two nodes [38].

4.3. Unsupervised Learning

With regard to the unsupervised machine learning algorithms, these include K-means clustering for identifying groups and iteration, factor analysis (FA), principal component analysis (PCA, to reduce dimensions), DBSCAN (density-based spatial clustering of applications with noise, which are used for data mining), and singular value decomposition (SVD) [19]. In unsupervised deep learning, the learning models such as self-organizing maps (SOMs); Boltzmann machines and AutoEncoders [39,40] are used to reduce dimensionality as the output is always 2-dimentional and is well-used. These allow the user to identify clusters of a specific type of input pattern [41]. The network of Boltzmann machines (or stochastic model) is a systematically connected neuron-like sampling learning algorithm and allows for interesting features in complex training data to be identified [42]. AutoEncoders are used in processing audio raw data into secondary vector space (e.g., word2vec) and have various variations such as spare AutoEndoders (allows a hidden layer and a reduction in overfitting), or contractive AutoEncoders (prevents overfitting and copying of values from hidden layers, add to the loss function), which are useful in terms of building the recommend systems or reducing dimensionality [35].

Unsupervised learning is useful for monitoring a system or building a binary recommend system. For example, it can be used to detect specific types of fraud. The key aspect of unsupervised learning is to unveil hidden patterns or groups from unlabeled large volumes of data, faster than supervised ML can do. Based on past purchase data, unsupervised ML can assist managers to identify trends in the data that can be used to plan a cross-selling strategy through add-on recommendations to customers during the check-out stage [43]. However, there are some aspects that need attention. Issues such as complexity in computation to train high volumes of data, and a lack of clarity as to which data were clustered and how the data were labeled. This means that users need time to understand the labeling and classifications, and interpretation. Unsupervised learning can be used for segmentation or understanding different customer groups, which helps managers to redefine their communication strategy better to fit the needs of certain groups and to monitor for fraudulent transactions or analyze the customer preference based on their search history [44].

4.4. Reinforcement Learning (RL)

Reinforcement learning (RL) models are either positive or negative based. The methods for RL such as SARSA (state-action-reward-state-action for learning Markov decision process policy), n-step method (the increment for rewards is estimated value of at time t, that incorporates n-step backup), actor–critic methods (or TD methods), and Q-learning [45]. Q-learning is value-based learning, which helps the agent (model) determine the optimal action within an environment. Examples of RL are in AlphaGo, Alpha Zero, Mario, Deepmind in Google data centers (with AI), self-driven car (with AI), and Keras in libraries [19]. RL can be applied widely such as self-driving in the automotive industry, for business strategy planning and data processing, but attention is needed in various aspects such as the parameters as this may affect the speed of learning.

Intuitive AI is an artificial natural network based on deep learning that can level up the result of analytics through the emulation of a wide range of human cognition and learning and the adaption of intuitively based understanding (e.g., Google's Deep mind (AI)). In AI development, there are different types of AI such as narrow AI is descriptive and performs one task at a time (answers are provided to the question of what happened); general AI, which is diagnostic (answers to comprehend the question of why did it happen) and makes a decision based on learning (independent); and predictive (answers to the question of what might happen next) [46,47]. Intuitive AI can identify anomalies in the dataset and make a deduction based on analyzed information, which, for example, helps to detect threats in financial services [46,47].

Some applications such as Replica, Sophia, Ellie, Nao, and Kasper recognize emotion and learn and adapt when interacting with humans. Empathy is an important ingredient in social interaction. Through the retailer deploying humanoid AI, they can manage the relationship with customers better as they can respond better to consumer requests by being able to detect the consumer's emotional state [48,49]. This can be looked upon positively as it represents a commitment to the customer centric approach and making the customer feel safe knowing that their needs are understood and that effort has gone into service their requirements, thus ensuring their expectations are met.

From the above, it can be noted that there are many different algorithms with different capabilities and functionalities, which associate with different levels of expert requirements and commitments. Table 1 is useful as it briefly outlines the different types of learning and their capabilities/functionalities and their application, especially in relation to DL. It provides a basic understanding to people who are enthusiastic in terms of using big data, but who have a limited knowledge of information technology and its application. Table 1 can be considered as useful with regard to answering questions such as:

(1) How should individuals make a decision as to what type of algorithm(s) is to be used or combined for the effective use of AI?
(2) What are the differences between supervised learning and unsupervised learning, and the implications regarding commitments vis-à-vis the expected quality outcome and the implication for implementation?
(3) Which aspects of the functionality of a system (e.g., mechanical, analytical or intuitive) should an individual focus on and why?

5. Improving Cyber Security through Utilizing AI

It can be argued therefore that various managers (e.g., marketing managers, logistics and distribution managers, and finance managers) will have knowledge of the use of AI, and will understand the benefits afforded by AI. Hence, it is possible for managers to relate the use of AI from advertising and product promotion to security awareness and counteracting fraud by making staff aware of the need to improve their security behavior. For example, Bresniker et al. [50] (p. 46) provided a number of insights into how AI can be used to aid the cyber security management process, especially from the stance of detecting threats and state: "AI/ML can drive down response times from hundreds of hours to seconds and scale analyst effectiveness from one or two incidents to thousands daily. With an adequate knowledge base, it can preserve corporate knowledge and use that knowledge to automate tasks and train new analysists".

Bresniker et al. [50] (p. 46) indicate that AI/ML will be increasingly used to:

1. Create pattern-matching tools that highlight security issues in networks;
2. Automate mundane tasks so that cyber security staff can use their time to respond to events in real time; and
3. Identify a range of threats and ensure that appropriate action is taken.

Bresniker et al. [50] provide a useful guide as to how AI/ML can enhance cyber security, however, in order for various managers in the organization to work together and provide an integrated approach toward strategic cyber security management [1], whereby the cyber security manager works closely with various other managers including the risk manager, the

business continuity manager, the IT manager, and the training manager, for example, it is necessary to match the human dimension of cyber security (e.g., identify human vulnerabilities) with the technical dimension of cyber security (e.g., identify technical vulnerabilities) through the application of the concept of sociocultural intelligence. The reason why matching is necessary is because fake news/disinformation is causing confusion and disruption and is likely to be weaponized further and used to complement various forms of cyber attack.

Fake news is well-orchestrated and targeted [51]. Petratos [52] (p. 764) draws on the United Nations definition and suggests that disinformation has been used "to confuse or manipulate people through delivering dishonest information to them". Bearing in mind that there has been an upward movement in ransomware attacks, managers need to realize that dealing with cyber criminals is not always as straight forward as expected. Drawing on the work of Greenberg, Tatar et al. [53] make known that a ransomware attack may be confused with data destruction malware whereby there is no possibility that the data would be made available to the target because the master boot records are in fact deleted by those carrying out the attack. It is for this reason that senior security managers within organizations need to develop a holistic approach to security because they may not be aware of the subtly behind disinformation. By accepting that disinformation detection requires a large investment in AI/ML, it should be possible for managers to develop resilience-based security by integrating cyber threat detection with security awareness.

6. Materials and Methods

To gain insights into how the concept of resilience can be embedded in the psyche of the organization so that it is a recognized component of the organization's memory, one of the researchers of this paper undertook a small group interview involving five highly knowledgeable organizational security experts. The experts were selected on the basis that they were knowledgeable in terms of strategic intelligence and were well able to place threat intelligence in the context of an organization's commitment to building resilience. The participants were all based in London and received permission from their employer to be involved in the research. Originally, it was envisaged that two small group interviews would be undertaken but it was not possible to organize two separate groups because those approached were busy and had commitments. Those that did attend and participate possessed operational knowledge that allowed them to offer unique insights into the topics under discussion [54] and uncover the underlying conditions [55]. In addition, they were known to have served in various senior security positions within an organization and were able to establish how intelligence and security could be integrated better so that security provision across business functions could be improved. The small group interview method was chosen because it allows for broad based questions to be asked that result in an open-ended group interview [56] (p. 17), whereby the participants can articulate their view, challenge and critique their peers, and then provide unique insights and solutions. Indeed, the selection of the group members (e.g., senior security professionals with work experience gained in both the private sector and the public sector) proved valuable in the sense that it was necessary to establish a group ethos [57] (p. 354) that allowed for meaning through reflection [9] (pp. 116–117). The small group interview was limited to one and a half hours and prior to the group interview commencing, the participants had agreed that the interview could be audio recorded. The researcher-facilitator agreed that specific comments made by individuals would not be attributed to the individuals concerned or the organization that they worked for. The group interview was framed so that the insights provided allowed for a holistic view of security to be derived that could then be interpreted from an organizational intelligence perspective. An interactive style was adopted during the small group interview, and this allowed each participant to explore the subject matter in the way they considered appropriate.

When undertaking a small group interview, it is important for the researcher to give attention to what the purpose of the group interview is and how the group members

relate to each other. For the purpose of this research, the objective was not to look at a basic set of conditions or derive insights in relation to government policy. The objective was to bring a highly experienced group of security experts together so that they could provide an in-depth understanding and appreciation of the topics discussed [58]. This was conducted by placing intelligence in the context of organizational resilience and at the same time, allowing each participant to gain intellectual satisfaction and knowledge in relation to perfecting their own organizational resilience policy. A semi-structured, open-ended approach was adopted as this allowed specific questions to be posed and provided the participants with some latitude to branch out and provide answers that incorporated real world examples.

In order to generate the required data, a number of questions were posed during the small group interview that included: How useful is the organizational learning concept in relation to the development of a security culture? How effective is transformational leadership in terms of the strategic intelligence approach? How can organizational vulnerabilities be eradicated through threat intelligence? The advantage of this approach is that the predetermined open-ended questions used were supplemented with additional questions that emerged as the interview progressed [59] (p. 315). The sub-questions that emerged were related to a range of topics that surfaced including crisis management, intelligence tools, networks, organizational skills, outsourcing, transformational leadership, trend analysis, trustworthy behavior, and risk management.

The data collection process was judged important in terms of the evidence and linking theory and practice. However, it was recognized that differences in regulatory conditions meant that senior security managers in one industry operated under different conditions compared to security managers in other industries. Although the view taken by the researchers was that the regulatory conditions exhibited differences, they were differences in degree only.

Immediately after the small group interview had been completed, the transcript was transcribed and then analyzed by the researchers. Each participant was provided with a copy of their portion of the transcript so that they could verify what they had said. Each participant, and indeed the facilitator, were assigned a number as names had not been used, and were identified accordingly. For the data analysis, the inductive approach was used whereby "the patterns, themes, and categories" were derived from the data as opposed to being imposed by the researchers before the data were collected [56] (p. 390). The main themes were identified and reported in [60]. In terms of the analysis of the data, we adapted the process associated with the grounded theory approach whereby we undertook open coding, axial coding, and selective coding [60], and developed a set of themes. The researchers then constructed a narrative in relation to each of the main themes. This would help the non-security specialist to understand how security practitioners placed threat intelligence in a sociocultural context from the perspective of enhancing an organization's resilience. This allowed the researchers to relate the main themes identified back to the intelligence cycle (IC) and critical thinking process (CTP) so that a cyber threat intelligence cycle process (CTICP) could be produced that was generic in nature and could be extended or adapted by managers in different industries.

7. Results

From the small group interview, it was clear that organizational learning, transformational leadership, organizational restructuring, crisis management, and corporate intelligence emerged as the main management considerations (themes) to be taken into account by top management because together, they provided insights into how threat intelligence was viewed and managed.

Organizational learning is viewed as important because it is a process whereby the mindsets of managers can be changed to embrace organizational values. In relation to how threats can be confronted and communicated to stakeholders, it is important for threat-based intelligence to be shared in real-time. As security covers a range of sensitive topics, it

is for this reason that staff are required to understand what trustworthy behavior is and why acts of benevolence are considered important and underpin relationship building. By establishing trust-based relationships, it is easier for individuals to share information when necessary and to safeguard themselves. This can be achieved by working within the organization's ethical code of conduct. Managers need to understand that the insider threat is continually evident, and the best approach appears to be for senior management to establish clearly defined security related roles that individuals can adopt when performing their duties. This means that security training needs to be formalized and a distinction made between training and education. The latter can be viewed as a higher level of knowledge attainment and inclusive of the understanding of what cyber threat intelligence (CTI) involves and how it is used on a day-to-day basis. Although not all staff need to be aware of the technical aspects of cyber security, those in positions of responsibility are required to have an all-round appreciation of the subject. In-house, formal cyber security awareness programs can be organized and administered on a continual basis to up-date staff and to make sure information technology staff talk with staff throughout the organization about security related issues. This should prove beneficial in terms of establishing and maintaining a security culture and ensuring that staff are aware of why and how they are to relate to law enforcement personnel when problems occur such as fraudulent practice, for example.

Transformational leadership was considered as a precursor of organizational change and is brought about through the implementation of strategic vision. Acknowledging that people can become complacent, it is necessary to ensure that people also do not become demotivated and lose sight of important considerations such as day-to-day security. However, transformational leadership is about establishing an organizational security culture, which should be viewed as a collectivist process. Another point that arose was that staff need to develop an understanding of the needs of people in other organizations. This will help staff to recognize symptoms such as corrupt practices and inefficiency in operations that could prove detrimental to the organization and its partners. Part of the transformational process involves staff using their own social network(s) to gain intelligence about cyber related attacks and centralizing this in the form of threat intelligence within a central command and control system within the organization. With regard to the security skill base of employees, managers need to ensure that security is defined in a certain way so that risk management is given adequate attention. To ensure that transformational leadership is effective, people within the organization that are viewed as supportive of security initiatives can adopt the role of champion of the cause and be given prominence to participate in in-house security seminars.

Organizational restructuring can result in an upheaval that places the organization at risk, especially when the management's attention is focused on other, non-security issues. Internal conflict can result in an organization becoming vulnerable because the type of uncertainty being dealt with relates more to an organization's internal situation than an outside threat penetrating the organization's defenses.

Crisis management is considered necessary because it can be assumed that at some point in time, the organization will be penetrated, and it is likely that other partner organizations will also be affected. Although essentially crisis management may be undertaken in different ways (e.g., depending upon the size and complexity of the organization), it must be noted that there are both direct and indirect influences involved. The organization's value system needs to support teamwork and requires that crisis management is viewed as an essential and combined process, whereby senior management make known to employees what a resilient organization is and how such an organization remains resilient. Areas often overlooked or underplayed include cyber insurance, and therefore the risk management process needs to be more formalized than it sometimes is.

Corporate intelligence is aided by the process of risk management and an area of attention is advances in biometrics, which covers threats brought about by fake IDs. Regarding the protection of the identity of employees, managers need to ensure that a person's

identity is always safeguarded and because information about an individual can be used against them, attention needs to be given to issues such as identity theft. This means that risk management is viewed from several perspectives and can also be related to human resource management policy and the recruitment of staff both from within the country and from abroad.

The findings from the small group interview highlight various issues that the cyber security manager needs to be aware of. These include the need to define what the organization's stance is in terms of security and resilience; and what the boundaries are that staff need to pay attention to when sharing information. These are important considerations with regard to how staff obtain data and information from outside the organization and share intelligence/knowledge with internal staff so that a cyber attack does not get through the organization's defenses. The quality of the data shared, and the way in which the data are shared, need to be given consideration in advance of a crisis occurring. During a crisis (e.g., an attack has penetrated the organization's defenses and staff struggle to deal with it in real-time), staff need to follow the policy laid down and ensure that cascading effects do not materialize.

Security awareness is, therefore, reflective of the investment in security training and education, however, it is recognized that more investment is needed in making staff aware of the consequences of an impact and convincing them that a proactive approach to gaining cyber security knowledge from appropriate sources is viewed as good practice.

8. Discussion

As well as placing emphasis on the quality of information/data derived from outside the organization, we also focus attention on the use of AI and whether managers can deploy supervised, semi supervised, or unsupervised algorithms for data analysis. This brings to attention whether managers have the knowledge required to interpret the results of the analysis (e.g., through human interpretation or machine interpretation) or whether a higher-level knowledge interpretation is required. Senior managers do need to invest time and effort into discussing these points and will need to put in place a protocol that provides guidance with regard to the analysis of big data. Acknowledging that sociocultural intelligence needs to be analyzed in a certain way and is dependent on the insights of experts brings to the fore the fact that managers need to consider the issue of resource availability.

The findings from the small group interview also highlight the need for a senior security manager/cyber security manager to adopt a transformational approach to security whereby threat analysis is an integral part of intelligence activity. By including current information pertaining to cyber threats, it is possible to highlight the need for cyber threat analysis to be viewed as necessary and to advocate a strategic cyber security management [1] approach. This will provide a basis for cyber security to be more widely appreciated than it is at present by managers that have a non-technical disposition. By adopting a more corporate intelligence focused approach to cyber security, whereby the lead organization takes greater responsibility for security, especially cyber security, guidance and support can be provided to the suppliers. Security staff, and the cyber security manager in particular, can promote the stakeholder view of security whereby supply chain partners take responsibility for updating their security and at the same time, pass threat intelligence data and information onto other stakeholders/network members. This will allow each stakeholder to coordinate their investment in cyber security [4]. The key point to note is that AI/ML can assist managers to undertake cyber threat intelligence (CTI), however, gaining permission across various supply chains is time consuming and requires negotiated access. This involves the sharing of sensitive data and information, and a commitment to building a sociocultural intelligence knowledge base.

To achieve linkage between security and intelligence, it is necessary to have an appropriate leadership model in place that embraces organizational learning and integrates the key aspects of the intelligence cycle (IC) with the critical thinking process (CTP) [9] (p. 139). The COVID-19 pandemic is continuing to have a lasting effect on the international econ-

omy, and evidence of this can be seen in the actions of unscrupulous individuals who are intent on exploiting health care provision [61]. By including issues such as fake news, identity theft, and ransomware, for example, in cyber threat intelligence (CTI), it is possible to establish how organized criminals are exploiting the market for legitimate drugs by engaging in online activities in relation to COVID-19 and the methods by which they gain financially. A question that arises is how can senior management devise a strategic approach to cyber security management that results in a collectivist appreciation whereby organizational partners pool resources to mitigate the risks identified? This is a question that top management appears to be discussing but the problem basically remains that not all business relationships are long-term in orientation. Opportunistic behavior may militate against a more structured and integrated approach to cyber security management across supply chains. Another issue that arises is, if partner organizations do not cooperate and share risk related data/information, how is a potential crisis to be effectively dealt with in real-time? Although the cyber security manager may focus on a specific type of cyber threat, it can be suggested that the scale of the problem means that it is necessary to utilize AI/ML to help counteract a range of cyber attacks.

It can be noted that AI is developing through time and its capability is to be viewed as several inter-locking AI and ML capabilities. By progressing from supervised to unsupervised learning and beyond, AI and ML assume a high level of decision-making that is freeing managers to invest time in strategy formulation as they are no longer required to undertake a lot of the analytical tasks themselves. Hence, it can be suggested that managers view the utilization of AI in terms of fostering the strategic capability of the organization and aiding business planning and resilience policy. To understand how AI is to be implemented requires strategic vision and a commitment to investing in a range of platforms (business platforms, enterprise platforms and enabling platforms) [62] that provide the company with a sustainable competitive advantage through relationship building.

Through establishing data-driven knowledge base construction, cyber security staff can guard against the problem of "inaccurate entity recognition and unreliable property/relation discovery due to insufficient training data" [63] (p. 11). In other words, it can be pointed out that cyber security specialists should work with those involved in cognitive sciences such as psychology to better understand how cyber security awareness and other areas of interest such as situational analysis can be incorporated more fully into the process of cyber threat intelligence (CTI) [17]. This should ensure that spikes of activism are noted and linked with disruptive geopolitical campaigns and specific types of hacking activity. Furthermore, emerging trends in fraudulent behavior may be linked to deteriorating economic conditions and the rise in criminal behavior, whereby organized criminal syndicates seek and exploit new market opportunities (e.g., fake websites linked to fictious products and services). Through converting information into intelligence and developing cyber security knowledge, a formalized approach to cyber threat intelligence (CTI) will materialize. Hence, threat actors need to be identified and categorized and this can be conducted by means of a threat template that outlines the opportunities in relation to the selected threat actors [64] (p. 6). By establishing the motivations of threat actors and linking through with their intended actions, it should be possible to understand the nature of the threat(s) and how matters escalate and an impact occurs [64] (p. 8).

Intra- and inter-company relationship building is important from the stance of sharing and utilizing threat-based data and information and can be considered as an integral part of cyber threat intelligence (CTI). Incident analysis tools exist [65] (p. 169) that can undergo further development that results in new initiatives in cyber security provision. It is also hoped that the sharing of such technology will encourage more dialogue between governments and a concerted effort will arise that results in a greater pooling of resources and cutting-edge joint research projects. The logic underpinning this view is to acknowledge that the pressures on managers to analyze big data will increase and new ways of detecting threats need to be found and implemented across industry sectors. Taking note of the risk associated with advanced persistent threats (APTs), it can be suggested that the incident

management process needs to be given increased attention. In addition, staff involved in cyber security need to have the confidence to question management practices and lobby for changes in company policy so that improved cyber security occurs at the same time as cyber threat intelligence (CTI) is upgraded.

Bearing the above in mind, we can reflect on the individual stages of the intelligence cycle (IC) and the critical thinking process (CTP) [9] (p. 139) and suggest that cyber threat intelligence (CTI) should be merged into the cyber threat intelligence cycle process (CTICP) so that the following stages are visible: (1) objective resilience (e.g., top management define resilience so that the organization is able to withstand a range of cyber attacks); (2) question framing (e.g., top management establish how the organization is to be made more resilient through human action and the combined usage of AI and ML); (3) threat intelligence (e.g., managers define what is involved and map the identified impacts against possible outcomes); (4) work tasks established (e.g., individual managers and experts are appointed to undertake specific tasks and roles); (5) collection of threat intelligence data and information (e.g., various research and data collection exercises are undertaken but mostly utilize AI and ML); (6) the analysis of threat intelligence data and information (e.g., cause and effect established/patterns in the data are identified that indicate a certain type of attack is occurring/is likely to occur); (7) interpretation of the results (e.g., risk register(s) up-dated within the organization and partner organizations); (8) dissemination of the results (e.g., the cyber security manager liaises with government bodies/agencies, trade associations and various resilience community groups and shares relevant industry information); (9) cyber threat intelligence (CTI) concepts/frameworks/models devised (e.g., industry specific and improved through additional evidence from university research group(s); (10) strategic cyber security management (e.g., assumptions are incorporated into a new way of thinking about the role that cyber security management plays); (11) reflection (e.g., staff focus on how advances in AI and ML will change the nature of future cyber threat intelligence (CTI) analysis and interpretation); and (12) intelligence culture (e.g., promotional activity undertaken within the partnership arrangement and more widely to help people in society prepare for cyber attacks and develop their own level of cyber security awareness so that they are better able to handle the psychological consequences of such attacks).

The benefits of such an approach are clear to see. The cyber security manager and various managers throughout the organization and its partners can utilize sociocultural intelligence to gain a more strategic view of the nature of cyber threats and how various cybers attacks are to be unleashed. The advantage of formalizing cyber threat intelligence (CTI) as opposed to viewing it as ad hoc is clear to see. Cyber threat intelligence (CTI) can be viewed from several stances including allowing "early detection of malicious behavior, preferably before a malicious actor gains a foothold in the network" and aiding the sense-making process by providing "insight into the relevant threat environment to decisionmakers" [66] (p. 301). Cyber threat intelligence (CTI) can therefore improve situational awareness and focus attention on key concerns such as how to guard against bias. Bias originates from cyber threat intelligence (CTI) feeds and/or analysis and can be linked to both criminal groups and state actors [66] (pp. 309–310). Bias is associated with the process itself whereby poisoning attacks occur as a result of training data, derived from open-source platforms, being manipulated/contaminated by malicious actors [67,68].

The cyber threat intelligence cycle process (CTICP) can help managers to identify how malicious actors are targeting organizations and how they are identifying future targets. This is conducted through the cooperation of designated managers, a commitment to using quality data and appropriate data analysis tools, and the sharing of intelligence on malicious actors and their networks. It is also envisaged that a range of ethical concerns will need to be addressed including data privacy, integrity and the accuracy of predictive intelligence [69]. By incorporating ethical issues and concerns into the process, it should be possible for managers to view predictive intelligence from the perspective of the changing needs of society, maintaining individual privacy and meeting legal challenges as and when

they occur. In addition, by embracing the sociocultural intelligence approach, the cyber security manager should be well placed to challenge and verify the patterns identified during the analysis of the big data.

9. Conclusions

For managers within an organization that are not familiar with AI to understand more fully what is involved when applying AI to help deal with cyber threats and to deal with cyber attacks when they occur, it is important to understand what cyber threat intelligence (CTI) is and how it feeds into strategic cyber security management [1]. Well-established intelligence concepts can be drawn on and modified to help the cyber security manager devise a cyber threat intelligence (CTI) blueprint that can be used to produce a more generic model or industry specific model, which is aimed at hardening the organization's defenses. By being committed to the use of situational analysis and embracing sociocultural intelligence inputs from external experts as well as in-house company staff, a security culture can be developed that has cyber security at the heart of it.

The advantage of placing cyber security at the center of security is that sociocultural intelligence can be reinforced by AI and in turn, AI can be monitored in terms of its ability to detect fake data and information and counter acts of data poisoning. The greater the quality of the data and the more sophisticated the process of analysis, the more the cyber security manager is able to work alongside colleagues to strengthen the organization's defenses. Through the process of integrating a number of separate but related tasks into a proactive stakeholder approach to cyber security management, the organization's supply chain will become more resilient and better able to withstand various forms of cyber attack.

10. Future Research

It is clear from the forgoing that a follow-up study can be undertaken that focuses more deeply on how AI/ML can enhance cyber security provision from the stance of a coordinated investment in cyber security from the organizations in a specific supply chain. This will provide insights into how organizations with a common trading mandate anticipate and guard against a possible cyber attack(s) and coordinate their defense [4]. The advantage of such a study is that it will provide evidence of a specific type of cyber threat intelligence (CTI) and outline how managers identify and organize supply chain resilience. Another research project that can be undertaken is to establish how managers overcome their lack of knowledge in relation to AI, and how they can develop relevant insights and/or contribute to the development of AI focused cyber security tools that lead to a better understanding of company–industry–society considerations and the need to ensure that AI is regulated appropriately [3] (p. 114). In addition, the insights into knowledge creation through various forms of learning [70] can be drawn on and placed more firmly in the context of managers understanding why network associations are important and how they can be developed through investment in AI.

It would also be appropriate to undertake research that contributes to cyber threat intelligence (CTI) methodology as this would help broaden the base of cyber threat intelligence (CTI) and solve a well-stated problem: "The volume and velocity with which new attacks are reported leads to a high daily influx of many single IoC datapoints that need further triangulation to assess their relevance to the specific threat context" [66] (p.304). Indeed, it should be possible to deploy soft systems methodology [71] and scenario planning [72] to link planning and modeling with strategy formulation and answer "what if" type questions that arise and once answered, enable initiatives in policy to be aimed at solutions to be found through learning.

Author Contributions: Conceptualization, Y.-I.L. and P.R.J.T.; Methodology, Y.-I.L. and P.R.J.T.; Formal analysis, Y.-I.L. and P.R.J.T.; Writing—original draft preparation, Y.-I.L. and P.R.J.T.; Writing—review and editing, Y.-I.L. and P.R.J.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to express their gratitude to the reviewers for their in-depth comments and suggestions for improving the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Trim, P.R.J.; Lee, Y.-I. *Strategic Cyber Security Management*; Routledge: London, UK; New York, NY, USA, 2022.
2. Abraham, C.; Sims, R.R. A comprehensive approach to cyber resilience. *MIT Sloan Manag. Rev.* **2021**, *63*, 1–4.
3. Wirkuttis, N.; Klein, H. Artificial intelligence in cybersecurity. *Cyber Intell. Secur.* **2017**, *1*, 103–119.
4. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* **2020**, *282*, 161–171. [CrossRef]
5. Rajan, R.; Rana, N.P.; Parameswar, N.; Dhir, S.; Sushil; Dwivedi, Y.K. Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technol. Forecast. Chang.* **2021**, *170*, 120872. [CrossRef]
6. Frith, C.D. The social brain? In *Social Intelligence: From Brain to Culture*; Emery, N., Clayton, N., Frith, C., Eds.; Oxford University Press: Oxford, UK, 2008; pp. 297–310.
7. Trim, P.R.J.; Lee, Y.-I. The Global Cyber Security Model: Counteracting cyber attacks through a resilient partnership arrangement. *Big Data Cogn. Comput.* **2021**, *5*, 32. [CrossRef]
8. Yamin, M.M.; Ullah, M.; Ullah, H.; Katt, B. Weaponized AI for cyber attacks. *J. Inf. Secur. Appl.* **2021**, *57*, 102722. [CrossRef]
9. Patton, K. *Sociocultural Intelligence: A New Discipline in Intelligence Studies*; The Continuum International Publishing Group: London, UK, 2010.
10. Hasan, K.; Shetty, S.; Ullah, S. Artificial intelligence empowered cyber threat detection and protection for power utilities. In Proceedings of the IEEE 5th International Conference on Collaboration and Internet Computing, Los Angeles, CA, USA, 12–14 December 2019; pp. 354–359.
11. Surya, L. An exploratory study of AI and Big Data, and it's future in the United States. *Int. J. Creat. Res. Thoughts* **2015**, *3*, 991–995.
12. Hagendorff, T.; Wezel, K. 15 Challenges for AI: Or what AI (currently) can't do. *AI Soc.* **2020**, *35*, 355–365. [CrossRef]
13. Gallese, V. Chapter 12: "Before and below 'theory of mind': Embedded simulation and the neural correlates of social cognition". In *Social Intelligence: From Brain to Culture*; Emery, N., Clayton, N., Frith, C., Eds.; Oxford University Press: Oxford, UK, 2008; pp. 279–296.
14. HSSAI. *Risk and Resilience: Exploring the Relationship*; Department of Homeland Security, Science and Technology Directorate: Arlington, MA, USA, 2010.
15. Argyris, C. *On Organizational Learning*; Blackwell Publishers Limited: Oxford, UK, 1996.
16. McCreight, R. Resilience as a goal and standard in emergency management. *J. Homel. Secur. Emerg. Manag.* **2009**, *7*, 1–7. [CrossRef]
17. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 1–13. [CrossRef]
18. Dawson, S. *Analysing Organisations*; Palgrave: Basingstoke, UK, 1996.
19. Ma, L.; Sun, B. Machine learning and AI in marketing—Connecting computing power to human insights. *Int. J. Res. Mark.* **2020**, *37*, 481–504. [CrossRef]
20. Salakhutdinov, R.; Hinton, G. Deep Boltzmann machines. In Proceedings of the 12th International Conference on Artificial Intelligence and Statistics (AISTATS), Clearwater Beach, FL, USA, 16–18 April 2009; pp. 2735–2742. [CrossRef]
21. Moerland, T.M.; Broekens, J.; Jonker, C.M. Emotion in reinforcement learning agents and robots: A survey. *Mach. Learn.* **2018**, *107*, 443–480. [CrossRef]
22. Jones, L. AI Trends in Retail, Retail & E-Commerce, 23 April. Available online: https://www.transperfect.com/blog/2021-ai-trends-retail (accessed on 15 June 2021).
23. Kohl's. 2020 Reimaging the Digital Shopping Experience with Snapchat. Available online: https://corporate.kohls.com/news/archive-/2020/august/reimagining-the-digital-shopping-experience-with-snapchat (accessed on 15 June 2021).
24. Roggeveen, A.L.; Grewal, D.; Karsberg, J.; Noble, S.M.; Nordfält, J.; Patrick, V.M.; Schweiger, E.; Soysal, G.; Dillard, A.; Cooper, N.; et al. Forging meaningful consumer-brand relationships through creative merchandise offerings and innovative merchandising strategies. *J. Retail.* **2021**, *97*, 81–98. [CrossRef]
25. Holzwarth, M.; Janiszewski, C.; Neumann, M.M. The influence of avatars on online consumer shopping behavior. *J. Mark.* **2006**, *70*, 19–36. [CrossRef]
26. Grewal, D.; Noble, S.M.; Roggeveen, A.L.; Nordfalt, J. The future of in-store technology. *J. Acad. Mark. Sci.* **2020**, *48*, 96–113. [CrossRef]

27. Roggeveen, A.L.; Sethuraman, R. Customer-interfacing retail technologies in 2020 & beyond: An integrative framework and research directions. *J. Retail.* **2020**, *96*, 299–309. [CrossRef]
28. Srikanth, A. Virtual Assistants vs Chatbots: What's the Differences & How to Choose the Right One? 2020, Freshdesk Blog. Available online: https://freshdesk.com/customer-engagement/virtual-assistant-chatbot-blog/ (accessed on 16 June 2021).
29. Croes, E.A.J.; Antheunis, M.L. Can we be friends with Mitsuku? A longitudinal study on the process of relationship formation between humans and a social chatbot. *J. Soc. Pers. Relatsh.* **2021**, *38*, 279–300. [CrossRef]
30. Skjuve, M.; Følstad, A.; Fostervold, K.I.; Brandtzaeg, P.B. My chatbot companion—A study of human-chatbot relationships. *Int. J. Hum. Comput. Stud.* **2021**, *149*, 102601. [CrossRef]
31. Campbell, C.; Sands, S.; Ferraro, C.; Tsao, H.Y.; Mavrommatis, A. From data to action: How marketers can leverage AI. *Bus. Horiz.* **2020**, *63*, 227–243. [CrossRef]
32. Huang, M.-H.; Rust, R.T. Artificial intelligence in service. *J. Serv. Res.* **2018**, *21*, 155–172. [CrossRef]
33. Kitchens, B.; Dobolyi, D.; Li, J.; Abbasi, A. Advanced customer analytics: Strategic value through integration of relationship-oriented big data. *J. Manag. Inf. Syst.* **2018**, *35*, 540–574. [CrossRef]
34. Vollrath, M.D.; Villegas, S.G. Avoiding digital marketing analytics myopia: Revisiting the customer decision journey as a strategic marketing framework. *J. Mark. Anal.* **2022**, *10*, 106–113. [CrossRef]
35. Gupta, R. Deep Learning Models—When Should You Use Them? From ANN to AutoEncoders, Towards Data Science, 2019, October. Available online: https://towardsdatascience.com/6-deep-learning-models-10d20afec175 (accessed on 18 June 2021).
36. IBM Cloud Education. Recurrent Neutral Networks, 2020, 14 September. Available online: https://www.ibm.com/cloud/learn/recurrent-neural-networks (accessed on 14 June 2021).
37. Wu, H.; Prasad, S. Semi-supervised deep learning using pseudo labels for hyperspectral image classification. *IEEE Trans. Image Process.* **2018**, *27*, 1259–1270. [CrossRef]
38. Ouali, Y.; Hudelot, C.; Tami, M. An Overview of Deep Semi-Supervised Learning. *arXiv* **2020**, arXiv:2006.05278. Available online: https://arxiv.org/abs/2006.05278 (accessed on 12 September 2022).
39. Manukian, H.; Pei, Y.R.; Bearden, S.R.B.; Di Ventra, M. Mode-Assisted unsupervised learning of restricted Boltzmann machines. *Commun. Phys.* **2020**, *3*, 105. [CrossRef]
40. Sakkari, M.; Zaied, M. A convolutional deep self-organizing map feature extraction for machine learning. *Multimed. Tools Appl.* **2020**, *79*, 19451–19470. [CrossRef]
41. Çelenk, U.; Ertuğrul, Ç.D.; Zontul, M.; Elçi, A.; Uçan, O. Dynamic Quota Calculation System (DQCS): Pricing and Quota Allocation of Telecom Customers via Data Mining Approaches. In *Handbook of Research on Contemporary Perspectives on Web-Based Systems*; Elçi, A., Ed.; IGI Global Publisher: Hershey, PA, USA, 2018. [CrossRef]
42. Hinton, G.E.; Sejnowski, T.J. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Washington, DC, USA, 19 June 1983; pp. 448–453.
43. IBM Cloud Education. Machin Leaning, 2020, 15 July. Available online: https://www.ibm.com/cloud/learn/machine-learning (accessed on 5 June 2021).
44. Gavrilova, Y. Artificial Intelligence vs. Machine Learning vs. Deep Learning: Essentials. 2020. Available online: https://serokell.io/blog/ai-ml-dl-difference (accessed on 15 June 2021).
45. Mnih, V.; Badia, A.P.; Mirza, M.; Harley, T.; Lillicrap, T.P.; Silver, D.; Kavukcuoglu, K. Asynchronous methods for deep reinforcement learning. *Int. Conf. Mach. Learn.* **2013**, *48*, 1928–1937. [CrossRef]
46. Gazit, M. The Fourth Generation of AI Is Here, and It's Called 'Artificial Intuitions' News, 3 September 2020. Available online: https://thenextweb.com/news/the-fourth-generation-of-ai-is-here-and-its-called-artificial-intuition (accessed on 17 June 2021).
47. Vector ITC. Fourth Generation of AI Arrives: Artificial Intuition, Vector ITC, 1 February. Available online: https://www.vectoritcgroup.com/en/tech-magazine-en/artificial-intelligence-en/fourth-generation-of-ai-arrives-artificial-intuition/ (accessed on 17 June 2021).
48. Yalçın, Ö.N.; DiPaola, S. Modeling Empathy: Building a Link between Affective and Cognitive Processes. *Artif. Intell. Rev.* **2020**, *53*, 2983–3006. [CrossRef]
49. Pizzi, G.; Scarpi, D.; Pantano, E. Artificial intelligence and the new forms of interaction: Who has the control when interacting with a chatbot? *J. Bus. Res.* **2020**, *129*, 878–890. [CrossRef]
50. Bresniker, K.; Gavrilovska, A.; Holt, J.; Milojicic, D.; Tran, T. Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. *Computer* **2019**, *52*, 45–52. [CrossRef]
51. Albright, J. Welcome to the era of fake news. *Media Commun.* **2017**, *5*, 87–89. [CrossRef]
52. Petratos, P.N. Misinformation, disinformation, and fake news: Cyber risks to business. *Bus. Horiz.* **2021**, *64*, 763–774. [CrossRef]
53. Tatar, U.; Nussbaum, B.; Gokce, Y.; Keskin, O.F. Digital force majeure: The Mondelez case, insurance, and the (un)certainty of attribution in cyberattacks. *Bus. Horiz.* **2021**, *64*, 775–785. [CrossRef]
54. Sinkovics, R.R.; Penz, E. Multilingual elite-interviews and software-based analysis: Problems and solutions based on CAQDAS. *Int. J. Mark. Res.* **2011**, *53*, 705–724. [CrossRef]
55. Easterby-Smith, M.; Thorpe, R. Research traditions in management learning. In *Management Learning: Integrating Perspectives in Theory and Practice*; Burgoyne, J., Reynolds, M., Eds.; Sage Publications: London, UK, 1997; pp. 38–53.
56. Patton, M.Q. *Qualitative Evaluation and Research Methods*; Sage Publications: London, UK; New Delhi, India, 1990.

57. Woods, P. Symbolic interaction: Theory and method. In *The Handbook of Qualitative Research in Education*; LeCompte, M.D., Millroy, W.L., Preissle, J., Eds.; Academic Press, Inc.: San Diego, CA, USA, 1992; pp. 337–404.
58. Frey, J.H.; Fontana, A. The group interview in social research. *Soc. Sci. J.* **1991**, *28*, 175–187. [CrossRef]
59. DiCicco-Bloom, B.; Crabtree, B.F. The qualitative research interview. *Med. Educ.* **2006**, *40*, 314–321. [CrossRef]
60. Strauss, A.; Corbin, J. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*; Sage Publications: London, UK, 1998.
61. Pawlicka, A.; Choraś, M.; Pawlicki, M.; Kozik, R. A$10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. *Bus. Horiz.* **2021**, *64*, 729–734. [CrossRef]
62. Carson, B.; Chakravarty, A.; Koh, K.; Thomas, R. *Platform Operating Model for the AI Bank of the Future*; Mckinsey & Company: London, UK, 2021; pp. 1–11.
63. Zhuang, Y.-T.; Wu, F.; Chen, C.; Pan, Y.-H. Challenges and opportunities: From big data to knowledge in AI2.0. *Front. Inf. Technol. Electron. Eng.* **2017**, *18*, 3–14. [CrossRef]
64. Meland, P.H.; Nesheim, A.A.; Bernsmed, K.; Sindre, G. Assessing cyber threats for storyless systems. *J. Inf. Secur. Appl.* **2022**, *64*, 103050. [CrossRef]
65. Settanni, G.; Skopik, F.; Shovgenya, Y.; Fiedler, R.; Carolan, M.; Conroy, D.; Boettinger, K.; Gall, M.; Brost, G.; Ponchel, C.; et al. A collaborative cyber incident management system for European interconnected critical infrastructures. *J. Inf. Secur. Appl.* **2017**, *34*, 166–182. [CrossRef]
66. Oosthoek, K.; Doerr, C. Cyber threat intelligence: A product without a process? *Int. J. Intell. Count.* **2021**, *34*, 300–315. [CrossRef]
67. Ranade, P.; Piplai, A.; Mittal, S.; Joshi, A.; Finin, T. Generating fake cyber threat intelligence using transformer-based models. In Proceedings of the International Joint Conference on Neural Networks, IEEE, Shenzhen, China, 18–22 July 2021; pp. 1–9. [CrossRef]
68. Khurana, N.; Mittal, S.; Joshi, A. Preventing poisoning attacks on AI based threat intelligence systems. In Proceedings of the IEEE 29 International Workshop on Machine Learning for Signal Processing Conference, IEEE, Pittsburgh, PA, USA, 13–16 October 2019. [CrossRef]
69. Tilimbe, J. Ethical implications of predictive risk intelligence. *ORBIT J.* **2019**, *2*, 1–28. [CrossRef]
70. Stella, M.; Kenett, Y.N. (Eds.) *Knowledge Modelling and Learning through Cognitive Networks*; MDPI: Basel, Switzerland, 2022. [CrossRef]
71. Checkland, P.; Scholes, J. *Soft Systems Methodology in Acton*; John Wiley & Sons: Chichester, UK, 2007.
72. Ringland, G. *Scenario Planning*; John Wiley & Sons: Chichester, UK, 2006.