Discussion of Spoofing Phenomenon: Distributed Emphasis Avoidance Networks with Social Distance and Velocity as Avoidance Systems for Information Health

Yasuko Kawahata †

Faculty of Sociology, Department of Media Sociology, Rikkyo University, 3-34-1 Nishi-Ikebukuro,Toshima-ku, Tokyo, 171-8501, JAPAN.

ykawahata@rikkyo.ac.jp,kawahata.lab3@damp.tottori-u.ac.jp

Abstract: This paper proposes a new mathematical model for understanding and addressing the risks of information Spoofing (unilateral supply of information:including Impersonation) in digital media. In today's society, the rapid development of digital media poses unprecedented challenges to information health. These include new risks such as filter bubbles and the spread of misinformation. These can negatively impact public risk perception and social decision-making, making it important to strengthen information immunity. The model applies the principles of self-organizing traffic accident avoidance systems based on biological problem-solving mechanisms to model the dynamics of risk information transfer and public risk perception in society. The three main components are as follows. Finally, the idea of an autonomous decentralized emphasis avoidance network algorithm was added to the discussion in this paper with the idea of adding a component that would allow the system to autonomously adjust the influence factor between risk and response, similar to how a vehicle in a traffic model adjusts its own behavior based on the behavior of neighboring vehicles. The idea is similar to how a vehicle in a traffic model adjusts its own behavior based on the behavior of neighboring vehicles. The model also calculates an impact coefficient for each risk at each time step and uses it to dynamically adjust the impact coefficient, aiming to stabilize the risk level toward a target level.

Keywords: Informational Health, Social Distance and Velocity, Spoofing:Impersonation in Digital Media, Misinformation and Public Perception, Self-Organizing Systems in Risk Management, Informational Immunity and Critical Thinking, Balancing Digital and Real-World Interactions, Dynamics of Risk Information Transmission, Informational Health in a Connected Society

1. Introduction

1.1 Spoofing:Impersonation and Gaslighting Associations and Risks an Informational Health Perspective Discussion

First, we will post regarding a perspective that has become a major issue in recent years in the discussion of informational health perspectives in this paper. The concept of spoofing has existed since the days when individuals attempted to deceive others by impersonating them. In the context of information and network security, spoofing attacks became a significant concern with the advent of the Internet and the increasing reliance on computer networks for communication.

The term itself has older roots in the context of jokes and deception, but as a technical term in cybersecurity it came into the limelight with the growth of the Internet and digital communication technologies. Spoofing attacks will become even more of a social problem in the future with the spread of AI and other technologies. Spoofing refers to passive accep-

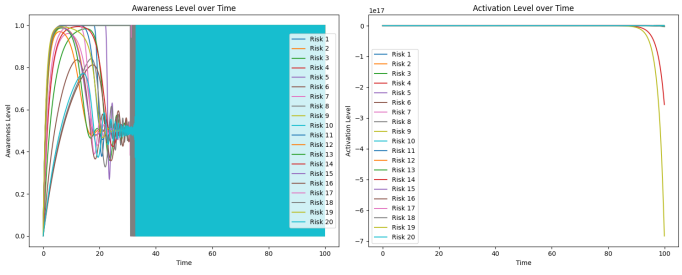

Fig. 1: Activation Level over Time Graph / Awareness Level over Time Graph

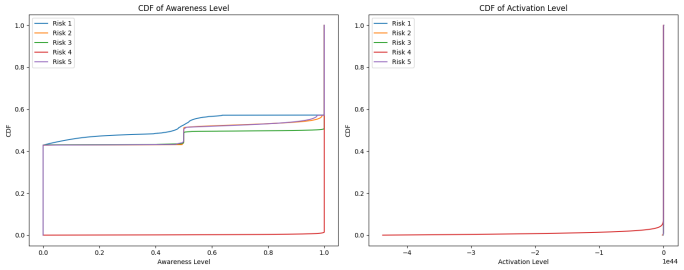

Fig. 2: CDF of Risk Level

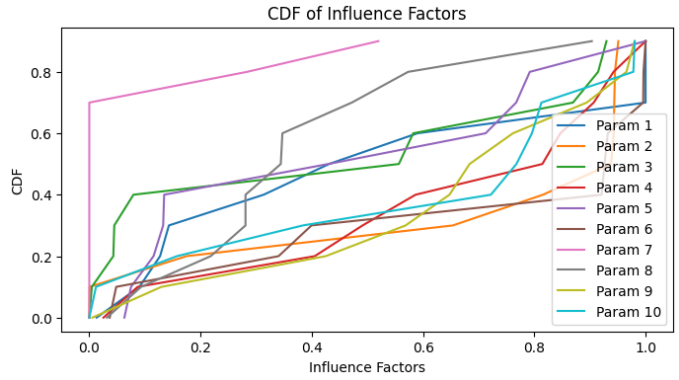

Fig. 3: CDF of Influence Factors

tance of information, lacking critical thinking and independent information retrieval. This phenomenon is particularly pronounced in the context of digital media, where users tend to rely on information provided unilaterally, and Gaslighting, whose relevance is discussed here, is a form of psychological manipulation in which victims are made to doubt their own judgment and memory. Media and information sources distort the facts, which may distort the recipient's perception of reality. Spoofing and gaslighting are interrelated in the way information is received. When Spoofing weakens critical thinking, psychological manipulation through gaslighting may be more effective. One-sided information supply reduces the ability of recipients to judge the truth or falsity of information, making them more susceptible to gaslighting. There are perspectives on the concern of declining informational health. Spoofing is a major threat to informational health. The diversity and quality of information is reduced and individuals risk making decisions based on all-encompassing and biased information. In particular, there is a significant risk of distorting perceptions of reality. Gaslighting can cause individuals to lose the ability to trust their own judgment and memory. This increases the credibility of disinformation and conspiracy theories in digital media and adversely affects the informational health of society as a whole. Both phenomena due to social and psychological influences can also undermine social cohesion and individual psychological stability. Decisions based on incorrect information can weaken social trust and negatively impact an individual's psychological health.

One possible countermeasure here is to promote critical thinking by strengthening critical thinking skills through education and media literacy programs. This will allow individuals to effectively evaluate the truth or falsity of information and increase their tolerance for gaslighting. It is important to maintain a diversity of information sources and not rely on a one-sided supply of information. Multiple perspectives reduce the risk of gaslighting and promote a more balanced understanding. And it is important that public awareness, i.e., media and educational institutions work to raise awareness of these issues to the general public. Society-wide understanding and cooperation is essential to maintaining informational health.

Spoofing and gaslighting can have significant consequences for informational health. Strengthening critical thinking, diversifying information sources, and raising public awareness are key to effectively addressing these risks. The advancement of digital media requires continued attention to and action on these issues.

1.2 Definition and Background of Spoofing

In the age of digital media, the risk of information Spoofing, or one-way supply of information, is attracting increasing attention. Spoofing refers to a situation in which the recipient does not actively search for information or think critically, but passively accepts the information given to him or her. With the proliferation of digital media, this phenomenon has become particularly pronounced.

In terms of the impact of the filter bubble, the concept of the "filter bubble" by Eli Pariser (2010) is a prime example of Spoofing. As information is customized online based on an individual's interests and past behavior, users are less exposed to diverse perspectives and information. This creates the risk that only biased information is provided. In terms of social media and the spread of disinformation, multiple studies on social media platforms reveal the rapid spread of disinformation and conspiracy theories. Users are often influenced by confirmation bias and tend to accept only information that reinforces their existing beliefs. This phenomenon can have a significant impact on public opinion formation and behavior. The importance of digital literacy perspective provides a way to address the risks of Spoofing. Improving critical thinking skills and educating people on how to evaluate information sources facilitates the transition from passive information reception to active information processing. Spoofing of information in digital media can have a profound impact on public health and social decision-making. Three research examples - filter bubbles, the proliferation of disinformation, and enhanced digital literacy - provide a deeper understanding of this problem and how to address it. It is clear that the development of the ability to process information actively and

critically, rather than passively accept it, is essential for the future of society. The proposed article aims to highlight the importance of analyzing the risks associated with Spoofing in the context of the outlined research methods and the relevance and significance of these methods. The underlying study focuses on a novel mathematical model that integrates principles of self-organizing traffic accident avoidance systems, inspired by biological problem-solving mechanisms, to effectively manage and communicate risk information in society. This approach is particularly relevant in today's digital age, where the constant flow of information can lead to challenges such as misinformation and filter bubbles.

Importance of Analyzing Spoofing Risks:

1. Informational Health:The model emphasizes informational health, acknowledging the risks in a digitally-dominated society. Spoofing information, or the unidirectional flow of information without critical engagement, can exacerbate misinformation and biased perceptions. Analyzing these risks is crucial for promoting a healthier information environment.

2. Risk Perception Dynamics:Understanding how spoonfed information shapes public risk perception is essential. The model's focus on the dynamics of risk information transmission and public reaction offers insights into the potential consequences of Spoofing in societal decision-making.

3. Misinformation and Biased Views:The culture of always-on connectivity increases the risks of misinformation. Analyzing Spoofing helps in developing strategies to enhance public ability to recognize and resist such misinformation.

In addition, the use of digital media highlights the importance of balancing relationships with those in the real world. Face-to-face communication promotes empathy, deeper understanding, and strengthens social connections. The interaction between digital media and the real world plays an important role in maintaining social connectedness and communal health.

This approach provides a framework for mathematical modeling of social and risk message risk with an emphasis on informational health. We provide a deep understanding of the impact of digital media and suggest strategies for maintaining social, psychological, and informational health. With informational health at the center of this approach, we aim to help the public respond more appropriately to risk and make sound, informed decisions. The model optimizes informational health by modeling the dynamics of risk information transmission and interpretation. It takes into account how risk messages are communicated and how they are interpreted and reacted to by the public and is based on three main components Risk Information Transfer Function (RITF), a function that evaluates how risk information is communicated in society and its effectiveness. It uses as parameters the clarity of the communication, its reach, and the comprehension of the receiver. 2. Risk Awareness Mechanism (RAM) determines how the public interprets and perceives risk information. It considers the accuracy, speed, and rate of translation of perceptions into action. Collaborative Risk Response Strategy (CRRS) is an approach to managing risk based on cooperation between different social groups. It includes as elements the level of cooperation between government, business, and civil society, the efficiency of communication, and shared resources.

The model dynamically simulates the interaction between the communication of risk information and the public's perception of risk as a self-organizing network. This approach allows us to understand how risk information circulates within society and impacts public health and safety.

Balancing Digital and Real-World Interactions: The study acknowledges the importance of face-to-face communication in promoting empathy and understanding. Analyzing Spoofing risks underscores the need for a balance, fostering healthy social connections both online and offline.

Informational Immunity: Enhancing informational health is akin to developing immunity against misinformation. This is particularly significant in the context of Spoofing, as it empowers individuals to discern and critically evaluate information.

Social and Psychological Health: The model's emphasis on social and psychological health in the face of digital media's impact is crucial. Analyzing Spoofing risks can contribute to strategies that maintain communal health and prevent social isolation.

Strategies for Risk Communication: The model offers a foundation for enhancing the effectiveness of risk communication. In terms of Spoofing, this implies developing communication strategies that promote critical thinking and informed decision-making.

In summary, the outlined mathematical model and its methods are highly relevant and significant in analyzing the risks associated with Spoofing in the digital age. By focusing on informational health, the dynamics of risk perception, and collaborative strategies, this approach offers a comprehensive framework to address the challenges posed by a constantly connected society and the unidirectional flow of information.

2. Related Research Cases

2.1 Spoof(Impersonation) Detection Systemss

Aakshi Mittal, Mohit Dua (2021) et al. built an impersonation detection system based on static-dynamic features and hybrid deep learning models in ASV. Spoofing detection is essential to improve the performance of current scenarios in automatic speaker verification (ASV) systems. By authorizing both the front-end and the back-end, a robust ASV system can be built. First, this paper compares the performance of

static and static-dynamic CQCC (Constant Q Cepstral Coefficients) front-end features by using LSTM (Long Short Term Memory) and time distributed wrapper models for the back-end. Second, a comparative analysis of ASV systems built using three deep learning models LSTM with Time Distributed Wrappers, LSTM and convolutional neural networks as backends, and static-dynamic CQCC features as frontends. Third, we discuss the implementation of two spoof detection systems for ASV by using the same static-dynamic CQCC features on the front end and different deep learning model combinations on the back end. The first of these two is a two-level spoofing detection system based on a voting protocol, using a CNN, LSTM model at the first level and an LSTM with Time Distributed Wrappers model at the second level. The second is a user identification and verification protocol, a two-level spoofing detection system, where the first level uses an LSTM model for user identification and the second level uses an LSTM model with Time Distributed Wrappers for verification. To implement the proposed study, a variation of the ASVspoof 2019 dataset was used, where all types of spoofing attacks such as speech synthesis (SS), speech conversion (VC), and replay were introduced into a single dataset. The results showed that on the front-end, static-dynamic CQCC features outperformed static CQCC features, and on the back-end, a hybrid combination of deep learning models improved the accuracy of the spoofing detection system. Akinori Ebihara, Kazuyuki Sakurai, and Hitoshi Imaoka (2019) proposed impersonation face detection based on singular and diffuse reflections in mobile devices. In this paper, we propose an efficient face presentation attack detection (PAD) algorithm that requires minimal hardware and a small database. The proposed algorithm utilizes a single monocular visible light camera and takes two face photos. The proposed $SpecDiff$ descriptor is constructed using two types of reflections: (i) specular reflections from the iris region, which have a specific intensity distribution dependent on liveness, and (ii) diffuse reflections from the entire face region, which represent the three-dimensional structure of the subject's face. SpecDiff descriptor The classifier trained with the SpecDiff descriptor outperformed other flash-based PAD algorithms in both the in-house database and the publicly available NUAA, Replay-Attack, and SiW databases. Furthermore, the proposed algorithm achieves statistically significantly better accuracy than end-to-end deep neural network classifiers while running about 6 times faster. In addition, the proposed algorithm achieves statistically significantly better accuracy than an end-to-end neural network classifier while running about 6 times faster. In this paper, we propose an efficient face presentation attack detection (PAD) algorithm that requires minimal hardware and a small database. The proposed algorithm utilizes a single monocular visible light camera and takes two face photos (one with flash and the other without flash). The proposed SpecDiff descriptors are constructed using two types of reflections: (i) specular reflections from the iris region, which have a specific intensity distribution depending on their liveliness, and (ii) diffuse reflections from the entire face region, which represent the 3D structure of the subject's face. The trained classifier outperformed other flash-based PAD algorithms in both in-house and publicly available NUAA, Replay-Attack, and SiW databases. Furthermore, the proposed algorithm achieves statistically significantly better accuracy than end-to-end deep neural network classifiers and is about 6 times faster in execution.Alejandro Gomez-Alanis, Antonio M. Peinado, José A. González,. Angel M. Gomez (2019) et al. built a robust impersonation detection Gated Recurrent Convolutional Neural Networks, an automatic speaker verification ASV system is exposed to spoofing attacks that can compromise its security. Anti-spoofing techniques have been studied mainly for clean scenarios, but have also been shown to perform poorly in noisy environments. In this study, we aim to improve the spoofing detection performance of ASVs in noiseless and noisy environments. To achieve this, we first propose the use of Gated Recurrent Convolutional Neural Networks GRCNNs as deep feature extractors to robustly represent speech signals as speech-level embeddings. Next, to increase the robustness of the system in noisy situations, we propose the use of S/N mask SNMs as new input features, which are almost immune to noise in the time-frequency domain of the input spectral features and should therefore be ignored when computing the embedding, to prevent spoofing inform the system. To evaluate our proposal, we experimented with clean and noisy versions of the ASVspoof 2015 corpus for detecting logical access attacks and the ASVspoof 2017 database for detecting replay attacks. for the ASVspoof 2019 corpus, we used the logical scenario and physical scenarios, we provide additional results including both. The experimental results show that our proposal clearly outperforms several well-known classical feature-based methods and other similar deep feature-based systems in both noiseless and noisy conditions. The problem of spoofing attacks that can affect automatic speaker verification (ASV) systems has received much attention in recent years, and many countermeasures have been developed to detect such high-tech attacks, such as speech synthesis and speech conversion. However, in noisy environments, the performance of anti-spoofing systems is significantly degraded. To address this problem, we propose a deep learning framework for extracting impersonation identity vectors as well as the use of soft missing data masks. The proposed feature extraction combines convolutional neural networks (CNNs) with recurrent neural networks (RNNs) to provide a single deep feature vector for each utterance. Thus, the CNN is treated as a convolutional feature extractor operating at the frame level; on top of the CNN output, the

RNN is employed to obtain a single spoofed identity representation of the entire utterance. Experimental evaluation on both clean and noisy versions of the ASVSpoof2015 corpus were conducted. Experimental results show that our proposal clearly outperforms other recently proposed methods, such as the popular CQCC+GMM system and other similar deep feature systems, in both noisy and noise-free conditions (2021).Spoofing : law, importance, and boundary work in futures trading Spoofing (canonically, "bidding or selling with the intent to cancel a bid or sale before execution") was once a skill that came in handy in face-to-face trading, but now suggests that it is a crime punishable by imprisonment. Guo-Rong Cai, Song-Zhi Su, Cheng-Cai Ling, Ji-Peng Wu, Yun-Dong Wu, and Shao-Zhi Li (2019), in Cover Patch: a general feature extraction strategy for spoof detection, focused on facial spoof prevention in security applications such as mobile payment and entry security. However, detection of spoofing by facial images is still a challenging task. Common image-based spoofing algorithms use global motion and texture information to distinguish whether an input face is real or fake. However, the performance of these methods is sensitive to changes in light and images acquired from different sensors. The main reason for this is that spoofed face images always have slightly different textures in localized areas, such as facial landmarks and salient regions. For this reason, this paper proposes a novel multi-patch feature extraction strategy to detect impersonation. First, we select a set of patches with a specific combinatorial scheme to cover the face image. Second, from these patches, features such as handcrafted gray-level co-occurrence matrices (GLCMs), local binary patterns (LBPs), and deep features are extracted. Third, all features are combined as a global descriptor of the face image and fed to the SVM classifier to validate the anti-spoofing detection. Experimental results show that the proposed strategy can effectively improve the performance on the accuracy of impersonation face detection in four widely used anti-spoofing databases. Heinrich Dinkel, Yanmin Qian, Kai Yu (2018) et al. (2018) study Raw Wave Deep Neural Networks for End-to-End Speaker Spoofing Detection in End-to-End Speaker Spoofing Detection, where malicious impersonation of an ASV system can lead to serious security breaches.An impersonation attack in the context of ASV is an attack in which a (potentially harmful) person alters or manipulates data in such a way that it is The term refers to a situation in which a (potentially harmful) person successfully impersonates another person already known to the ASV system by falsifying or manipulating data. While most prior work has focused on enhanced spoof recognition capabilities, end-to-end models are a potential alternative. In this paper, we investigate the training of deep convolutional, long-short memory (LSTM), and vanilla neural network raw wave frontends and analyze the effects of frame size, number of output neurons, and sequence length on their suitability for spoofing detection.A coupled convolutional LSTM neural network (CLDNN) is proposed, outperforming previous attempts on the BTAS2016 dataset (0.82% $rightarrow$ 0.19% HTER) and positioned as the current state-of-the-art model for the dataset. Demonstrating that the end-to-end approach is suitable for the critical replay detection task and that the proposed model can distinguish between device-independent spoofing attempts, for the ASVspoof2015 dataset, the end-to-end solution outperforms previous attempts for the S1-S9 conditions with a 0.00% equal error rate (EER) was achieved. We show that an end-to-end approach based on raw waveform input can outperform common sepral features without using context-dependent frame expansion. We also evaluate cross-database (domain mismatch) scenarios and show that the proposed CLDNN model trained on the BTAS2016 dataset achieves an EER of 25.7% on the ASVspoof2015 dataset. (2018) et al. describe spoofing detection in automatic speaker matching systems using DNN classifiers and dynamic acoustic features Many spoofing countermeasures have been developed to improve the security of ASV systems. In the front-end domain, much research has been done to find effective features that can distinguish spoofed speech from authentic speech, and results have been published showing that dynamic features are more effective than static features. In the back-end domain, Gaussian Mixture Models (GMMs) and Deep Neural Networks (DNNs) are the two most common classifiers used for spoofing detection. The log-likelihood ratio (LLR), generated from the difference between the log-likelihood of a human and an impersonator, is used as the impersonation detection score. In this paper, we train a 5-layer DNN impersonation detection classifier using dynamic acoustic features and propose a new simple scoring method that uses only the human log likelihood (HLL) for impersonation detection. In particular, we mathematically prove that the new HLL scoring method is better suited for the spoof detection task than the traditional LLR scoring method, especially when the spoofed speech is very similar to human speech; in combination with the DNN-HLL method, we propose five different dynamic filter bank-based cepstral features and the performance of Constant Q Cepstral Coefficients (CQCC) were extensively investigated. Experimental results show that compared to the GMM-LLR method, the DNN-HLL method can significantly improve the accuracy of spoofing detection; compared to the CQCC-based GMM-LLR baseline, the proposed DNN-HLL model reduces the average equal error rate for all attack types to 0.045%; and compared to the GMM-LLR baseline, the proposed DNN-HLL model reduces the average error rate for all attack types to 0.045%, outperforms the performance of the previously presented approach for the ASVspoof 2015 challenge task.Integrating the CQCC-based DNN-HLL impersonation detection system with the ASV system can sig-

nificantly reduce the false positive rate of impersonation attacks. Jianlin Guo, Yancheng Zhao, Haoran Wang (2023) et al. Generalized spoofing detection and incremental algorithm recognition in voice spoofing have caused much debate, e.g., artificial intelligence-based software can be used by anyone to generate nude photos and deep-fake images can be generated automatically. This poses a major threat to both individuals and society. In addition to video and image forgery, audio forgery also poses many dangers, but not enough attention has been paid to it. Furthermore, existing research focuses only on the detection of voice forgery and ignores the identification of forgery algorithms. In traceability, recognizing algorithms that synthesize spoofed speech is of great value. In this study, we propose a system that combines speech spoofing detection and algorithm recognition. On the other hand, we discuss the generalizability of the spoofing detection model in terms of embedding space and decision boundaries to deal with speech spoofing attacks generated by spoofing algorithms that are not in the training set. We present a voice spoofing algorithm recognition method based on incremental learning that takes into account data flow scenarios in which new spoofing algorithms continue to emerge in reality; experimental results on the ASVspoof LA dataset show that our system improves the generalizability of spoofing detection, and that it can be used to detect spoofing attacks in a real-world setting, shown to be able to identify new voice spoofing algorithms without catastrophic forgetting. (2020) et al. validate a new face spoofing DB with capture angles and distances. However, spoofing attacks threaten the security of facial biometric systems by generating false faces. Therefore, considering only advanced spoofing cases such as 3D masks is undesirable because it requires additional equipment and increases the cost of implementation. To prevent easy spoofing attacks using printouts and displays, a two-dimensional (2D) image analysis method using existing face recognition systems is appropriate. Therefore, we proposed a new database "Pattern Recognition Spoofing Advanced Database" to prevent spoofing attacks based on 2D image analysis. This database is the first face spoofing database that takes angle and distance variations into account. Therefore, it can learn various positions of faces and cameras. To validate the effectiveness of this database, various experiments were conducted, and the accuracy of this database in detecting impersonation using ResNet-18 was 96.75%. Experimental results in various scenarios showed that pinch-angle images, close-range images, and replay attacks had better spoofing detection performance than frontal images, far-range images, and print attacks, respectively. In addition, cross-database validation results showed that the performance of training on this DB and then validating on other databases (DBs) was better than vice versa. The results of cross-device validation by camera type showed little difference, and it was concluded that the type of image sensor did not affect detection accuracy. The results confirm that the proposed DB, which takes into account various distances, shooting angles, lighting conditions, and backgrounds, can be used as a training DB for detecting impersonation attacks in general face recognition systems. Jonathan N. Blakely, Shawn D. Pethel (2022) et al. Quantum Limits for Classical Spoofing with Electromagnetic Signals Spoofing with electromagnetic signals requires measuring their properties and preparing a spoofed signal whose copy is sufficient to fool the receiver. A classic application of spoofing is radar, where an airborne target attempts to evade tracking by ground radar by emitting pulses that indicate false distance and speed. In one scenario, it was shown that sensors can detect spoofing at the single-photon level using quantum mechanics. Here we analyze an idealized spoofing scenario in which the transmitting/receiving pair attempting to detect spoofing utilizes a signal randomly selected from a set of non-orthogonal coherent states. We show that a spoofer that makes optimal use of classical information about the state of the transmitted signal (the best measurement and preparation strategies allowed by quantum mechanics) will inevitably emit an incomplete spoof, which the receiver can use to reveal the presence of the spoofer or to identify the true reflection and spoof. Importantly, we show that the quantum limit on classical spoofs is still important, even in regions where the average photon number is large. Aoki (2022) et al. describe the detection of spoofing attacks in a face recognition system using a visual transducer with patchwise data expansion. In this paper, we propose an impersonation attack detection method using the Vision Transformer (ViT), which extracts features based on patches to extract fine features in face images. To improve the accuracy of spoofing attack detection, we also propose a patch-by-patch data augmentation.Kristiawan Nugroho and Edy Winarno (2022) use a deep neural network algorithm to detect spoofing of fake speech. In particular, spoofing is a problem that must be solved because of the possibility of using false voices, such as voice spoofing and fraud. Various classification methods in data mining have been used in research to detect spoofing. However, low accuracy, especially in managing large data sets, has been an obstacle to using this approach. Deep neural networks (DNNs) are a deep learning technique often used in studies that process large amounts of data; DNN approaches have proven to have excellent performance. In this study, the DNN approach is used to detect the authenticity of a speaker's voice. The results show that DNN is an excellent method for detecting spoofed voices with a model accuracy of 96.5%, precision of 97.3%, recall of 96.5%, and F1 measure of 96.7%.Mari Ganesh Kumar, Suvidha Rupesh Kumar, Saranya M. S , B. Bharathi, Hema A. Murthy (2019), Spoof Detection Using Time-Delay Shallow Neural Network and Feature Switching to detect spoofed speech is a suggested that it is a funda-

mental problem. Spoofing can be done by logical access, such as speech synthesis or speech transformation, or by physical access, such as playback of pre-recorded utterances. Inspired by state-of-the-art x-vector-based speaker verification approaches, this paper proposes a time-delay shallow neural network (TD-SNN) for impersonation detection for both logical and physical accesses. The novelty of the proposed TD-SNN system over conventional DNN systems is its ability to handle variable-length utterances during testing. The performance of the proposed TD-SNN system and the baseline Gaussian Mixture Model (GMM) is analyzed on the ASV-spoof-2019 dataset. The performance of the system is measured by the minimum normalized tandem detection cost function (min-t-DCF). When examined by individual features, the TD-SNN system consistently outperforms the GMM system for physical access. For logical access, the GMM outperforms the TD-SNN system on certain individual features. When combined with the decision-level feature switching (DLFS) paradigm, the best TD-SNN system outperformed the best baseline GMM system on the evaluation data, with relative improvements of 48.03% and 49.47% for both logical and physical access, respectively. The most common method deployed by hackers is to target end-to-end technology and exploit human weaknesses. Social engineering and spoofing are examples of these approaches. One approach to carrying out these attacks is to use malicious Uniform Resource Locators (URLs) to deceive users. Finding harmful Uniform Resource Locators (URLs) is difficult but a fascinating problem because phishers typically generate URLs randomly, so researchers must detect them while keeping in mind the underlying behavior of the spoofed URLs that are generated. This study describes an approach for identifying spoofed Web sites using machine learning techniques that analyze different aspects of benign and spoofed URLs. We examine how address bar-based features, anomalous features, and HTML and Java-based elements can be used to detect spoofed websites.Rahul T. P, P. R. Aravind, Ranjith C, Usamath Nechiyil, Nandakumar Paramparambath (2020) et al. Verify voice spoofing using deep convolutional neural networks with transfer learning. Some spoofing attacks, such as replay attacks, are easy to implement but very difficult to detect, requiring appropriate countermeasures. In this paper, we propose a deep convolutional neural network based speech classifier to detect spoofing attacks. The proposed method uses the acoustic time-frequency representation of the power spectral density of the mel frequency scale (mel spectrogram) through deep residual learning (adaptation of the ResNet-34 architecture). Using a single model system, an equal error rate (EER) of 0.9056% and 5.32% was achieved on the evaluation data set for the logical access scenario, and an equal error rate (EER) of 5.87% was achieved. For the ASVspoof 2019 physical access scenario, the evaluation dataset was 87% for development and 5.74% for the evaluation dataset.Caller ID spoofing is a global industry problem and often a significant source of telephone fraud. To address this problem, the Federal Communications Commission (FCC) has mandated that U.S. carriers implement STIR/SHAKEN, an industry-driven solution based on digital signatures. but extending this PKI to the global telecommunications industry would be extremely difficult, if not impossible. Furthermore, it only works with SIP (VoIP) systems, leaving traditional SS7 (landline and cell phone) systems unprotected. So far, alternatives to STIR/SHAKEN have not been adequately studied. This paper proposes a PKI-less solution to combat caller ID spoofing: caller ID verification (CIV). CIV authenticates caller ID based on a challenge-response process instead of a digital signature. CIV supports both SIP and SS7 systems. Perhaps counterintuitively, we show that number spoofing, in combination with Dual-Tone Multi-Frequency (DTMF), can be leveraged to efficiently implement the challenge response process. We implement CIV for VoIP, cellular, and landline phones across heterogeneous networks (SS7/SIP) by simply updating the software on the user's phone. This is the first caller ID authentication solution in current telecom architecture with a working prototype for all three types of phone systems. Finally, we show how CIV implementation can be optimized by integrating CIV as a service into the telecom cloud. Unknown Authors (2023) et al. Spoofing Against Spoofing: (2023) et al. Spoofing Against Spoofing: Towards Caller ID Verification in Heterogeneous Communication Systems Caller ID spoofing is a global industry problem and often acts as a significant trigger for telephone fraud. To address this problem, the Federal Communications Commission (FCC) has mandated that U.S. carriers implement STIR/SHAKEN, an industry-driven solution based on digital signatures. STIR/SHAKEN relies on a public key infrastructure (PKI) to manage digital certificates but extending this PKI to the global telecommunications industry would be extremely difficult, if not impossible. Furthermore, it only works with SIP (VoIP) systems, leaving traditional SS7 (landline and cell phone) systems unprotected. So far, alternatives to STIR/SHAKEN have not been adequately studied. This paper proposes a PKI-less solution to combat caller ID spoofing: caller ID verification (CIV). CIV authenticates caller ID based on a challenge-response process instead of a digital signature. CIV supports both SIP and SS7 systems. Perhaps counterintuitively, we show that number spoofing, in combination with Dual-Tone Multi-Frequency (DTMF), can be leveraged to efficiently implement the challenge response process. We implement CIV for VoIP, cellular, and landline phones across heterogeneous networks (SS7/SIP) by simply updating the software on the user's phone. This is the first caller ID authentication solution in current telecom architecture with a working prototype for all three types of phone

systems. Finally, we show how CIV implementation can be optimized by integrating CIV as a service into the telecom cloud. Detecting Spoofing Attacks in Face Recognition Systems Spoofing attacks that use visual transducers with patch-wise data augmentation are a serious threat to face recognition systems by malicious third parties because face images can be easily collected from the Internet. In this paper, we propose a spoofing attack detection method using the Vision Transformer (ViT), which extracts features based on patches to extract fine features in face images. We also propose a patch-by-patch data augmentation to improve the accuracy of spoofing attack detection. The effectiveness of the proposed method is demonstrated through accuracy evaluation experiments using public datasets. In this paper, we propose a deep neural network algorithm to detect spoofed speech. In particular, spoofing is a problem that must be solved because of the possibility of using fake voice, such as voice spoofing and fraud. Various classification methods in data mining have been used in research to detect spoofing. However, low accuracy, especially in managing large data sets, has been an obstacle to using this approach. Deep neural networks (DNNs) are a deep learning technique often used in studies that process large amounts of data; DNN approaches have proven to have excellent performance. In this study, the DNN approach is used in detecting the authenticity of a speaker's voice. The results show that DNN is an excellent method for detecting spoofed voices with a model accuracy of 96.5%, precision of 97.3%, recall of 96.5%, and F1 measure of 96.7%. Su-Kyung Yoo, Seo-Wi Kim, Kun-Ha Suh, and Yui-Cheol Lee (2020), et al. used DenseNet for face spoofing detection. However, face recognition is a biometric technique that is vulnerable to impersonation. Types of spoofing attacks include printing, replay, 3D masking, etc. Recently, face spoofing detection methods based on learned features using convolutional neural network series have been introduced, In this paper, face spoofing detection using DenseNet-121 was studied. For performance measurements, we used CASIA-FASD and the lab-generated PR-FSAD. The results can be attributed to the structural feature that DenseNet-121 well reflects the broadband frequency characteristics of images. Swathika Swathika Ravindran, Geetha (2021) et al. Overview of Spoof Detection in ASV Systems In recent years, speech-based applications have been widely used in various applications for speaker recognition. Currently, there is a wide range of expertise in analyzing spoofing and anti-spoofing in automatic speaker verification (ASV) systems Current advances in ASV systems have led to an interest in protecting these speech biometric systems for real-world applications The following is a brief overview of the current state of the art in the field of anti-poofing analysis. This paper provides literature on spoofing detection, novel acoustic feature representations, deep learning, and end-to-end systems. In addition, we summarize prior work on spoofing attacks with an emphasis on SS, VC, and replay, as well as recent efforts in spoofed speech detection and countermeasure development for speech impairment tasks. In 2018 research, face spoofing detection based on color distortion has been identified as a realistic challenge for securing face recognition systems against spoofing attacks. Spoofing attacks are performed by printing or displaying a digital image of the captured target (target user) in front of the sensor. These extra reproduction steps cause color distortion between the facial artifact and the actual face. This study addresses the problem of spoof detection by modeling the radiometric distortions produced by the recapture process. The spoofing detection process utilizes registration data and is followed by face identification. Once identified, color transformations between observed and registered faces are computed. A compact parametric representation is proposed to model these radiometric transformations and is used as a feature for classification. The proposed method is evaluated in the public databases of Replay-Attack, CASIA, and MSU, and its superiority over state-of-the-art measures is demonstrated. The limitations of the proposed method are clearly identified and discussed through experiments in hostile evaluation conditions, where color distortions are generated not only by the recapture process but also by natural illumination changes.2021 In the study Spoofprint: A New Paradigm for Spoofing Attacks Detection, with the development of voice spoofing technology, voice spoofing attacks have become one of the main threats to automatic speaker verification (ASV) systems. Traditionally, researchers have tended to treat this problem as a binary classification task. Binary classifiers are typically trained using machine learning (including deep learning) algorithms to determine whether a given speech clip is genuine or spoofed. This approach is effective in detecting spoofing attacks generated by known audio spoofing techniques. However, in real-world scenarios, new types of spoofing techniques are rapidly emerging. Since it is not possible to include all spoofing techniques in the training data set, it is desirable that the detection system be able to generalize to unknown spoofing techniques. In this study, we propose a new paradigm for spoofing attack detection called Spoofprint, which instead of using a binary classifier to detect spoofed audio, uses a paradigm similar to the ASV system and includes a registration phase and a verification phase. We evaluate the performance on the original and noisy versions of the ASVspoof 2019 Logical Access (LA) dataset. Results show that the proposed Spoofprint paradigm is effective in detecting unknown types of attacks and often outperforms state-of-the-art techniques. Wang Shen, Jie Liu, Min He, Wenjin Wang (2019) et al. unsupervised face impersonation prevention used in dual camera based feature matching is an important part of face recognition systems to protect subjects' privacy and life safety. Most current face impersonation prevention

algorithms are based on feature extraction and machine learning. The performance of machine learning-based approaches depends on the quantity and quality of training data. In this paper, we propose an unsupervised face impersonation prevention method based on dual-camera feature extraction and matching that does not require offline learning.The principle of the proposed method is simple, intuitive, and generally applicable. The core idea of the method is to exploit the fact that 3D faces have different feature representations in images from two cameras with different viewing angles compared to 2D impersonated faces (faces printed on paper or projected on a screen). The proposed method was benchmarked on a dataset created by our dual-camera setup and showed 94.2% accuracy. The quality of artificially generated speech has improved significantly with the development of speech synthesis and speech conversion technologies, and in practical applications such as automatic speaker verification (ASV), detection of spoofed speech is extremely important in practical applications such as automatic speaker verification (ASV). Modern neural network-based spoof detection models can effectively distinguish between most artificial and natural speech in the latest ASVspoof 2019 evaluation. Motivated by recent advances in adversarial example generation, this paper studies the robustness of neural network-based voice spoofing detectors against adversarial attacks. To this end, we propose an adversarial post-processing network (APN) that post-processes the speech waveforms generated by a baseline speech conversion system to generate adversarial examples against a white-box anti-spoofing model. Experimental results demonstrate the adversarial capability of the proposed APN against the white-box anti-spoofing model, which was used as the adversarial target of the APN during the training phase. For example, the equal error rate (EER) of the fusion detection model based on the light convolutional neural network (LCNN) increased from 0.278% to 12.743% under white-box conditions without degrading the subjective quality of the converted speech. Furthermore, the trained APNs are able to compete against detectors with unseen structures or unseen features by improving the EER. All of these results indicate that adversarial voice generation poses a threat to the performance of state-of-the-art spoofing detection models. Yong Wang, Zhuoyi Su (2019) et al. proposed a method to detect voice transform spoofing in dense convolutional networks. Therefore, it is very important to distinguish spoofed speech from authentic speech. Much of the current research focuses on voice conversion (VC), synthesis, and recapture to mimic the target speaker in order to break through ASV systems by increasing the misrecognition rate. However, another type of spoofing exists: voice transformation (VT). This transforms the speech signal so that it is "unrecognizable," increasing the false rejection rate; VT has not received much attention, and it is often used to impersonate a target speaker in order to increase the false rejection rate. Therefore, this paper surveys models of VTs and proposes a method for detecting spoofed speech by VTs from authentic speech using a very deep convolutional network consisting of 135 layers. In this paper, we examine the model of VT and propose a method to detect spoofed speech by VT from authentic speech using a very deep convolutional network of 135 layers. Experimental results show that the average accuracy within and across databases outperforms reported state-of-the-art methods. Zhang You, Jiang Fei, and Zhiyao Duan (2020) et al. described one-class learning in synthetic speech impersonation detection. In recent years, researchers have developed anti-spoofing techniques to improve the reliability of ASV systems against spoofing attacks. However, most techniques have difficulty detecting unknown attacks, which often have a different statistical distribution than known attacks. In particular, the rapid development of synthetic voice spoofing algorithms is generating increasingly powerful attacks, putting ASV systems at risk of unknown attacks. In this study, we propose an anti-spoofing system that uses one-class learning to detect unknown synthetic speech spoofing attacks (speech synthesis and speech conversion). The key idea is to compact the authentic speech representation and inject an angular margin to separate spoofing attacks in the embedding space. Without resorting to data augmentation methods, our proposed system outperforms all existing single systems (i.e., those without model ensembles), achieving an equal error rate (EER) of 2.19% on the evaluation set of the ASVspoof 2019 Challenge logical access scenario, Yuxiang Zhang, Wenchao Wang and Pengyuan Zhang (2021) et al. Effects of silence and dual-band fusion in anti-spoofing systems, Current neural network-based anti-spoofing systems are less robust. Its performance further degrades after speech activity detection (VAD) is performed, making it difficult to apply in practice. In this study, we investigated the effects of silence at the beginning and end of speech and found that differences in silence are part of the criteria for determining countermeasures. We also examined the causes of performance degradation due to VADs. Experimental results showed that the neural network loses information about the silence after the silence is removed by the VAD operation. This could lead to more severe overfitting. To solve the overfitting problem, this paper also analyzes the causes of overfitting of the system from different frequency subbands. The results show that the high-frequency portion of the features is the main cause of system overfitting, while the low-frequency portion is more robust but less accurate against known attacks. Therefore, we propose a dual-band fusion anti-spoofing algorithm. This algorithm requires only two subsystems, but outperforms all but one primary system submitted for the ASVspoof 2019 Challenge logical access condition. Our system has an EER of 3.50% even after VAD operations, suggesting that it is

feasible for practical use.

2.2 Risk Communication and Media

Previous Research Case Studies (2021) in 'Health Risk Communication and Media' describe that Risk communication is a concept defined by many organizations like World Health Organization (WHO) and Centers for Disease Control and Prevention (CDC). Effective risk communication is a complex process. It is an interactive process of exchange of information and opinion among individuals, groups, and institutions. Risk communication is part of the risk management process, with the primary aims to promote awareness and understanding of risks. In the risk management process, risk communication is at the center. There are a number of approaches to the process of risk communication and its components, including how messages are sent and received. The management of public health outbreaks has always included a specific communication component in the form of warnings, risk messages, evacuation notifications, messages regarding self-efficacy, information regarding symptoms, and medical treatment, among many others. Media can play a significant role for raising awareness of the health issues. But the difficulty is to find the right channel of communication for the target audience. Additionally, Previous Research Case Studies (2016) in 'Risk Communication and Risk Dialogue' describe that Risk communication serves different objectives depending on the specific circumstances of the risk considered and the aims of communicators. Under emergency and crisis conditions the aim is to provide timely, honest and useful information to the public notably in order to enable potentially exposed people to protect themselves, reduce the uncertainties and the deriving anxiety and stress and prevent behaviour that might aggravate the risks or increase the damage or costs incurred. In such cases, the information is mostly unidirectional, but collecting feedback is important in order to assess how the information is received and understood. Modern risk communication as part of the regulatory process is instead conceived as a two ways process involving in a sustained dialogue, through appropriate stages and procedures, all the relevant partners, managers, assessors, stakeholders, the public and decision makers. The objective is to adequately inform the decision-making process, integrate the societal dimensions of risk into the appraisal, ensure transparency and accountability and prepare the conditions for the effective implementation of risk management measures. The EU has set out procedures for stakeholder and public consultation, during both the risk assessment and the risk management stages. In particular, EFSA and the Commission Scientific Committees have internal rules on public consultation at various stages of their assessment activities. Moreover, the Commission has established consultation principles and guidelines, as part of its Better Regulation guidelines, which apply to all major initiatives including regulatory proposals and decisions on risks. Additionally, Previous Research Case Studies (1997) in 'Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks [Book Review]' describe that Review(s) of: Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks, by Regina Lundgren Columbus: Batelle Press, 1995, ISBN 0935470-76-X, 175+xii Pages. Additionally, Previous Research Case Studies (2016) in 'of Risk Communication' describe that The conveyance of technical risk information from experts to the lay public is unlikely to be successful unless the social context of such messages is addressed. This context includes social networks, economic resources, political rights and responsibilities, histories, and ideologies. Social context can be taken into account by clearly defining desired outcomes, identifying the information desired by citizens, and choosing communicators carefully. Technical and social perspectives on risk communication, incomplete in themselves, can in combination improve management of hazards. The emerging field of risk communication has emphasized the meaningful conveyance of technical information from risk experts to laypeople. This paper argues that the social context of risk communication is just as important, and sometimes more important, than the technical issues with which the field has largely been concerned. Messages are ultimately conveyed from person to person; what and how risk messages are received will be affected by our relations with the communicator, other humans, and the material artifacts concerned. Although the importance of social context has been "recognized," this recognition has been relatively superficial. A first approximation of "social context" is compared here to the current emphasis in risk communication. The examples used in this article deal with hazardous waste, hazardous facility siting, and natural disasters, but the arguments made apply as well to other hazards (e.g., radon, occupational safety and health). The focus is on how lay receivers of risk messages are affected by social context, but the influence of social context on the construction of risk messages is also important.1 Tasks for risk communicators which combine the technical and social context approaches are suggested, and some barriers to the use of risk communication based on social context are briefly noted. Additionally, Previous Research Case Studies (2011) in 'Risk communication in public health.' describe that Risk communication has been defined as a two-way exchange of information between interested parties about the nature, significance and/or control of a risk. In public health, this means that engaging the audience and responding to questions and concerns is equally as important as delivering key public health messages. The strategies used for communicating risk are based on the level of hazard a particular risk poses as well as the level of public concern or 'outrage' about that hazard. For example, a health

risk may be low but subject to high levels of public concern and media attention. Additionally, Previous Research Case Studies (2016) in 'Communicating Health Risks to the Public : A Global Perspective' describe that This book reviews current health risk communication strategies, and examines and assesses the technical and psycho-sociological tools available to support risk communication plans. It brings together approaches to risk communication from a number of countries and describes the techniques, including drama, storytelling and scenarios that are used to identify and prioritise key communication issues, and to identify policy responses. The book also provides a review of the methods and tools available for risk assessment, risk communication and priority setting, which are relevant not only to practitioners but to health planning more generally, and to many other areas of public health and policy. The discussion of these techniques is supported by case studies, and is concluded by a chapter reflecting on the conceptual and research issues that still need to be addressed. It also proposes new directions for risk communication that key into the public imagination with the aim of gaining their trust and confidence in the risk messages. Communicating Health Risks to the Public: A Global Perspective brings together a wide variety of perspectives on risk communication, from the perspectives of health, anthropology, psychology, and media. It should be of interest not only to those involved in risk assessment or communication but to anyone interested in the role of science and the media in the political process. Additionally, Previous Research Case Studies (2013) in 'Risk Communication: The Communication of Cost- Effectiveness Studies of Anti-Malaria Interventions to Policy Makers' describe that Risk Communication This section discusses issues related to risk communication across a range of publicly perceived highrisk industries (such as pharmaceuticals, nuclear, oil, etc.). It reports critically and provides analysis on risk communication as an outcome of risk research within these industries. Contributions are intended to include methods working towards the advancement of risk perception research and describe any lessons learned for successfully communicating to the public about risk. Additionally, Previous Research Case Studies (2020) in 'The Evolving Field of Risk Communication' describe that The 40th Anniversary of the Society for Risk Analysis presents an apt time to step back and review the field of risk communication. In this review, we first evaluate recent debates over the field's current state and future directions. Our takeaway is that efforts to settle on a single, generic version of what constitutes risk communication will be less productive than an open-minded exploration of the multiple forms that comprise today's vibrant interdisciplinary field. We then review a selection of prominent cognitive, cultural, and social risk communication scholarship appearing in the published literature since 2010. Studies on trust in risk communication messengers continued to figure prominently, while new research directions emerged on the opportunities and critical challenges of enhancing transparency and using social media. Research on message attributes explored how conceptual insights particularly relating to framing, affective and emotional responses, and uncertainty might be operationalized to improve message effectiveness. Studies consistently demonstrated the importance of evaluation and how varying single attributes alone is unlikely to achieve desired results. Research on risk communication audiences advanced on risk perception and multiway engagement with notable interest in personal factors such as gender, race, age, and political orientation. We conclude by arguing that the field's interdisciplinary tradition should be further nurtured to drive the next evolutionary phase of risk communication research. Additionally, Previous Research Case Studies (2004) in 'Risk communication, risk perception, and public health.' describe that Risk communication is about building trust while deploying an interactive and ongoing communication process in which audience members are active participants. This interactive participation may not solve a public health crisis, but it will help reduce unwarranted fear, anxiety and distrust. Consequently, if a government agency fails to understand how to effectively communicate about health risks, their trustworthiness and credibility may suffer, and a crisis event may go from bad to worse. Language: en Additionally, Previous Research Case Studies (2021) in 'Risk communication and COVID-19 in Europe: lessons for future public health crises' describe that Risk communication is key to engaging with the public on non-pharmaceutical interventions (NPIs) to promote acceptance, compliance and policy support. This article outlines the considerations neede... Additionally, Previous Research Case Studies (2019) in 'Communicating Radiation Risk: The Power of Planned, Persuasive Messaging.' describe that Every day, health physicists and physicians are expected to communicate effectively with concerned people, but rarely (if ever) are they given training on how to effectively communicate. In an age of social media, this paper presents the relevance of teachings from an ancient Greek philosopher. Aristotle's Rhetoric is still considered one of the most influential works on persuasive messaging. He puts the onus of effective communications on the people with the "true" and "just" information to communicate that information clearly to the audience. By communicating with intention-using the persuasive appeals of ethos, pathos, logos, and storytelling-radiation professionals can speak to their expertise in radiation science, while adapting their instructions, presentations, and communication styles to meet the needs of each type of audience: from scientists to concerned citizens, from doctors to first responders, and beyond. Additionally, Previous Research Case Studies (2020) in 'Ethical aspects of risk communication' describe that The essence of risk communication

is to provide patients with a clear understanding of the benefits, harms, trade-offs and uncertainties of any proposed treatment. Doctors often assume that they do this well, but often overestimate the numeracy among even well-educated patients. Because doctors and patients make complex decisions using both intuitive and deliberative thinking, there are hidden sources of bias in decision-making on both sides. Recent research suggests that patients are best equipped to understand risk when they are simply able to 'get the gist' of the risk involved in their treatment. This can be achieved by a process of thinking out loud in which the doctor outlines the factors that they think might be important to the individual patient, checking carefully for shared understanding along the way. Risk communication should be based on up-to-date knowledge, honesty, empathy and respect. Additionally, Previous Research Case Studies (2007) in 'Learning and teaching about risk communication' describe that [Extract] Risk communication is a fundamental skill in the consultation between health professionals and patients. Such communication is part of the process leading to shared decision-making and involves the clinician discussing advantages and disadvantages of treatment, while specific numerical data about potential outcomes may be given.[1] Risk communication is the open two-way exchange of information and opinion about risk, which should lead to better understanding and better decisions about clinical management.[2] This exchange of information and opinion is important if treatment decisions are to reflect the attitudes to risk of the patients who will live with the outcomes.[3] Informed consent to investigations or treatment is impossible without an understanding of risk. Good risk communication reduces the possibility of litigation. Additionally, Previous Research Case Studies (2020) in 'Best Practice Risk Communication and Conclusion' describe that This chapter concludes the book. In Chap. 1, this book set out to explore the role of power and expertise in risk communication about public health and safety as it relates to policy making. We examined current debates around expertise in Chap. 2 and used these to critique the social amplification of risk framework from the power perspective in Chap. 3. The policy evaluation risk communication framework was central to this study (see Adekola 2018). Thus, in this book, we used the Policy Evaluation Risk Communication framework to analyse three public health risk debates (the smoking, MMR vaccine and sugar debates in the UK) to investigate the roles that power and expertise have played in shaping these debates (see Chaps. 4, 5 and 6). Further discussion and cross-case analysis of the empirical findings was carried out in Chap. 7 and the study's empirical findings were then used to advance existing conceptualisation of the social amplification of risk framework, in Chap. 8. Additionally, Previous Research Case Studies (2020) in 'Risk, Risk Communication and Policymaking' describe that This is the first and introduction chapter of the book. This chapter sets out the background of the study and situates this within the literature on risk and risk communication. It highlights the book's perspective on risk and risk communication, and the aim of the book, which ultimately is to understand how power and expertise in risk communication about public health and safety relate to policymaking. The core aim of the book is to examine social amplification of risk in policymaking—how an argument within a set of risk arguments, becomes amplified in a policy context. Additionally, Previous Research Case Studies (2020) in '[Risk communication in healthcare: literature review and recommendations for clinical practice].' describe that Consistent with the principles of evidence-based medicine, communicating clinical risks to patients and their families is an essential part of informed consent and decision-making. Communication of clinical risks can take place during and after consultations, orally or in writing, based on the latest available scientific data, when available. Numerous studies show that there are different degrees of innumeracy in the general population, meaning more or less significant difficulties mastering numbers in everyday situations. It is therefore imperative to communicate risks in a way that is adapted to the patients' variable numeracy and health literacy levels. This article presents a synthesis of international research on risk communication, as well as recommendations for clinical practice. Additionally, Previous Research Case Studies (2012) in 'Health Risk Communication' describe that Health risk communication deals with planned or unplanned communication to the public about the nature, impact and management of a wide array of health threats, such as cancer, HIV/AIDS or influenza pandemics.Traditional health risk communication models used to stress a one-way flow of healh risk messages to the public. The dominant focus was on experts (government, health organizations,...) merely dissiminating risk information and educating a ?lay' and ?ignorant' public about health threats. However, this simplistic top-down model of communication ignored the complex nature of the audience and the public's understanding of risk information. Fortunately, there has been a shift away from topdown communication about health threats. By the late 1990's new models of risk communication have arisen that advocate an approach to risk communication as a two-way process or an interaction between the communicator and the audience. Rather than stressing education of a passive public, such perspective focuses on risk communication as a dialogue or as a dynamic exchange of information.Essential to the undestanding of risk communication as an interactive process is the view that risk has both objective and subjective qualities. The public's understanding of a health risk is not purely a matter of appraising the objective probability of a health threat or its consequences, but also the result of a more subjective and value-laden evaluation. The public can perceive

health risks in complex and multi-faceted ways: different individuals may perceive risks differently because they may appraise the relevance of the risk differently, they may value the consequences of the threat differently or they may rate the threat differently on a set of other attributes or dimensions. This modern formulation of risk as a subjective social construct has triggered a wide range of questions about how public understanding of health risks and health risk messages can be colored by social, cultural and psychological influences. As such it has also opened the door to studying risk communication as an interactive process.Summarizing, the interactive perspective on health risk communication moves beyond the old view of a passive reciever and instead focuses on how health risk messages can elicit different responses dependent on (a) who communicates them, (b) how they are communicated and (c) how the public actively processes the information. In the last decade there have been several advances in research investigating these three areas of health risk communication.Concerning the source of the message, it has become evident that mass media play a pivotal role in communicating information about health threats and in shaping perceptions of health risks. For instance, a large scale study on health news and the American public by the Kaiser Family Foundation and the Harvard School of Public Health found that four in ten adults followed health news stories closely (1). A number of studies have looked at how media affect public perceptions and attitudes about health risks and related behaviors (2,3). Others have examined how the media and the public have responded to recent health crises, such as the H5N1 virus or Severe Acute Respiratory Syndrome (SARS) (4). In addition, there is a growing recognition of the role of information source characteristics, such as the extent to which the public trusts the messenger or the perceived credibility of the source. It is likely that, no matter what the risk information is or how the message is presented, health care professionals, scientists, press or government officials will not succeed in communicating health risks effectively if they do not meet up to the public's expectations.Regarding message presentation, there is growing evidence that the effectiveness of health risk messages is highly dependent on how these messages are constructed or framed. Traditional approaches to health risk communication were based on the assumption that the public rationally evaluates health threat messages. . . . Additionally, Previous Research Case Studies (2016) in 'Communicating risks to patients and the public' describe that It is well known from everyday life that communication is difficult. However, it is an even greater challenge to communicate sensitive or controversial issues such as risks in particular in emotional situations. Consequently, risk communication is much more than just talking about an issue. It requires specific knowledge, tailoring and targeting information to the patient's needs and abilities, and observing communication rules. The most frequent mistake is underestimating the need for specific skills and ignoring the pitfalls and dos and don'ts of risk communication. The basic information is given and demonstrated by various examples. Additionally, Previous Research Case Studies (2017) in 'Health Risk Perception and Risk Communication' describe that Risk perceptions are a prerequisite for protective action. Both scientists and practitioners need to understand the multifaceted nature of health risk perception and risk communication. This article Additionally, Previous Research Case Studies (2017) in 'Breaking Bad News in the High-concern, Low Trust Setting: How to Get Your Story Heard.' describe that "BREAKING BAD NEWS" or communicating risk information to a worried audience is a challenging yet crucial task. When the chips are down and people are worried, there will be information overload with many sources screaming for attention. In this cacophony, officials must adopt special evidence-based techniques in order for the truth and helpful information to be heard (Hyer and Covello 2007). The perception of the health risk from radiation consistently produces some of the highest levels of concern by the general public. Exact health risk information is often hard to obtain. Sensational media attention often greatly increases anxiety. Policymakers with little or no specific training or expertise in risk and crisis communication often charge into the arena (Ropeik 2011). A basic premise of this article is that communicating risk information about radiation—with the reinforcing goals of building or repairing trust, informing and educating people, and gaining agreement about appropriate actions and behaviors—requires a sophisticated scientific approach using best practices of risk communication (Covello 2011a). Risk and crisis communication are scientific disciplines with over 8,000 peer-reviewed publications and 2,000 books printed, along with reviews of the literature by the National Academy of Sciences and other preeminent bodies. Essentially risk and crisis communication involve connecting with people who have an activated brain limbic system or amygdala (emotional and "fight or flight response"). This natural emotional response makes it very difficult to present detailed information in a logical fashion. Neurological studies using the latest brain-imaging techniques demonstrate a clear effect of emotions on altering risk-based decision-making processes. Effective risk communication has three primary goals: to build or repair trust, to inform stakeholders about the risk, and to gain agreement (e.g., agreement about what is needed) (Covello et al. 1989). First and foremost is to build and repair trust. In the public eye, the subject of radiation consistently elicits some of the strongest levels of fear and anxiety. Trust is the absolute currency of effective risk communication. Establishing and maintaining trust is, thus, paramount for effectively connecting and delivering useful information about radiation. To gain trust, one must express true empathy—"people want to

know you care before they care what you know." Studies show that listening, showing compassion, and demonstrating empathy contribute over half to peoples' perception of trust. What is alarming is that this trust is assessed in as little as 9–30 s. Factors such as one's competence and expertise contribute a mere 15–20% of perceived trust, with honesty and openness another 15–20%, and all other factors filling in the remainder. When attempting to connect with people in a high concern, low-trust setting, one must first and foremost demonstrate empathy and compassion before the audience will hear anything else. Additionally, Previous Research Case Studies (1998) in 'Risk communication: A handbook for communicating environmental, safety, and health risks. Second edition' describe that The essential handbook for effectively communicating environmental, safety, and health risks, fully revised and updated Now in its sixth edition, Risk Communication has proven to be a valuable resource for environmental, safety, and health professionals who are tasked with the responsibility of understanding how to apply the most current approaches to communicating risk and debunking misinformation. The sixth edition updates the text with fresh and illustrative examples, lessons learned, and recent research as well as provides advice and guidelines for communicating risk information. Previous Research Case Studies include background information to understand the basic theories and practices of risk communication and explain how to plan an effective strategy and put it into action. The book also contains data on evaluating risk communication efforts and explores how to communicate risk during and after a health or environmental emergency. Risk Communication brings together in one resource proven scientific research with practical, hands-on guidance from risk practitioners with over 30 years of experience in the field. This important guide: Provides new examples of communication plans in government and industry, the depiction of probability, methods of working with news media, and use of social media Contains a new chapter on partnerships which covers topics such as assigning roles and expectations, ending partnerships, and more Includes information on Americans with Disability Act laws, particularly Sections 504 and 508 that deal with electronic tools Presents real-world case studies with key lessons all risk communicators can apply. Written for engineers, scientists, professors and students, land use planners, public health practitioners, communication specialists, consultants, and regulators, the revised sixth edition of Risk Communication is the must-have guide for professionals who communicate risks. Introduction – Approaches to communicating risk – Laws that mandate risk communication – Constraints to effective risk communication – Ethical issues – Principles of risk communication – Determine purpose and objectives – Analyze your audience – Develop your message – Determine the appropriate methods – Set a schedule – Develop a communication plan – Information materials – Visual representations of risks – Face-to-face communication – News media – Stakeholder participation – Technology-assisted communication – Social media – Partnerships – Evaluation of risk communication efforts – Emergency risk communication – International risk communication – Public health campaigns. Additionally, Previous Research Case Studies (2016) in 'Risk Communication: An Integral Element in Public Health Emergencies.' describe that DEAR EDITOR, Over the years, multiple number of health emergencies (such as disease-outbreaks – H1N1 or Ebola disease, chemical accidents, radiation leaks, natural disasters, conflicts, wars, etc.), have been reported worldwide, which have claimed the lives of thousands of people.However, in most of the instances the mental sufferings can be avoided, or lives of susceptible people can be saved, provided the local population had access to fast, effective and transparent communication.In fact, realizing the scope of risk communication in preventing disease, disability, and even mortality, it has been considered as one of the eight integral functions, which the World Health Organization (WHO) member states must develop to effectively respond to both public health emergencies and humanitarian crises. In general, risk communication refers to the real-time exchange of information, advice and opinions between experts and masses exposed to the threat, which can compromise their survival, health, economic or social well-being.The primary objective of effective risk communication is to enable people at risk to take well-informed decisions not only to protect themselves, but even their loved ones from the emergency by taking appropriate and timely protective and preventive actions.However, the success of risk communication is eventually dependant on thorough understanding of people's (in terms of their knowledge, practices, perceptions, concerns, beliefs, etc.); experts attributes (such as their credibility, caring and empathic nature, level of trust between experts and affected persons, etc.); and ability of the communicator to promptly detect the prevalent rumors/myths/misconceptions and address them before it starts interfering with the preventive and control measures.Risk communication has been acknowledged as one of the lifesaving intervention, especially in public health emergencies.This is so because people do have a right to know how to protect themselves and their relatives' health by understanding and adopting protective behaviors by taking well-informed decisions.Furthermore, the communication at times of emergencies has even benefited other stakeholders like local program managers (in assessing health impact of the emergencies and providing them evidence to develop an effective health response), donors and concerned public across the globe.In addition, at times of emergencies, effective risk communication can empower nations/local communities to preserve their socioeconomic and political stability, and even prevent the loss of trust of people

on public health authorities by enabling health officials to address people's concerns and needs so that relevant and acceptable advice can be communicated to the masses.A wide range of communication techniques (viz., mass media, social networking, etc.) have been adopted to facilitate risk communication.However, a wide range of challenges such as globalization; extensive international trade and travel; a complex animal-human interface; rise in threat of bioterrorism; enormous popularity of the social networking sites (because of which the reliance on health experts/authorities has seriously decreased, and at the same time it even encourages spread of rumors and incorrect information); and changes in the field of journalism (like 24-h journalism where most of the news consists of opinions rather than facts) and approach of journalists, have been identified which have seriously questioned the effectiveness of risk communication.In the modern world, the need of the hour is to strengthen the existing risk communication capacity so that the existing challenges and the health emergencies can be tackled better.The primary strategy is to implement the WHO guidelines released to cover different aspects of risk communication.This includes components such as establishing a comprehensive policy and plans for risk communication; ensuring training of the health professionals/local officials so that they can acquire appropriate skills and be competent; conducting training sessions for journalists on how to report on health emergencies; devising a mechanism to discourage people to advertise incomplete or wrong information on social networking websites; and running simulation exercises to assess the extent of preparedness of nations.In addition, the approach to constitute an Emergency Communications Network (ECN) system with an aim to identify, train, assess and deploy risk communication experts also deserves immense significance, so that the members (who have the ability to work in coordination with national and local authorities) of the network can be deployed at times of emergencies.In fact, since the constitution of ECN, the members have been deployed in disease outbreak settings, humanitarian emergencies and in natural disasters.To conclude, risk communication is an integral element of any public health emergency response and thus all efforts should be taken by the nations to strengthen the same, so that lives of numerous people can be saved at times of emergencies. Additionally, Previous Research Case Studies (2018) in 'Developing Health Risk Communications: Four Lessons Learned' describe that In this chapter, we summarize our research on the development of health risk communications and focus on four lessons we have learned from doing so: (1) Effective communications must be accessible and actionable to the intended audience; (2) effective communications must use an appropriate delivery method; (3) effective communications must be pretested and evaluated prior to wide-scale rollout; and (4) effective communication design and evaluation requires interdisciplinary teams. While the examples provided in this chapter focus on the health domain, we believe that the four lessons outlined here will be helpful to those who wish to implement effective risk communications to a wide range of target audiences on a broad set of applied topics. Additionally, Previous Research Case Studies (1992) in 'Risk Communication: An Emerging Area of Health Communication Research' describe that (1992). Risk Communication: An Emerging Area of Health Communication Research. Annals of the International Communication Association: Vol. 15, Communication Yearbook 15, pp. 359-373. Additionally, Previous Research Case Studies (2011) in 'Risk communication, radiation, and radiological emergencies: strategies, tools, and techniques.' describe that Risk communication is the two-way exchange of information about risks, including risks associated with radiation and radiological events. The risk communication literature contains a broad range of strategies for overcoming the psychological, sociological, and cultural factors that create public misperceptions and misunderstandings about risks. These strategies help radiation risk communicators overcome the challenges posed by three basic observations about people under stress: (1) people under stress typically want to know that you care before they care about what you know; (2) people under stress typically have difficulty hearing, understanding, and remembering information; (3) people under stress typically focus more on negative information than positive information.

2.3 Risk Communication and Media

Amin Hosseini, Gergana Jostova, Alexander Philipov, and Robert Savickas (2020), Social Media Risk Premium, social media has become part of Main Street and Wall Street reality. Diversifying social media risk is difficult. This is because social media risk is a trigger for contagion, with certain issues "going viral" and affecting a wide range of companies. Institutional and individual investors have shown that they demand a risk premium for stocks and bonds with high social media beta. Unlike other risk factors whose origins are difficult to pinpoint, social media risk is associated only with the social media era and did not exist prior to the rise of today's social media behemoths. The annual risk premium for social media risk is 7.2% for stocks and 3.3% for bonds.Ateeq Ahmad (2013) states that social media security risk and protection in a security attack is one of the most pressing information technology issues facing any business today but it is particularly concerning for small and medium-sized businesses, where finding the resources needed to protect against the ever-increasing security risks is becoming increasingly difficult and complex. Social media platforms such as Twitter, Facebook, and LinkedIn are increasingly used by businesses to engage with customers, build brands, and communicate to the world. For companies, there are real risks associated

with the use of social media, ranging from brand damage to leakage of confidential information. The fundamental objective of this paper is to protect systems from unauthorized social media attacks. Brenda K. Wiederhold (2013) notes, "In times of disaster, social media has the power to save lives...The Third International Conference on Disaster and Risk (Davos), held in May and June 2010, highlighted the role of information and communications technology (ICT) in the early detection of natural disasters. According to conference statistics, after any natural disaster, it took only 30 minutes to assess the damage using social media. Conference participants emphasized the need to get the news out to government leaders and first responders in time for successful evacuation from disaster-prone areas. Conference participants declared that the "legality of social media is an institutional issue, not a technical one" and urged attendees representing their countries to develop policies, stating that the role of this effective communication channel during the chaos of a disaster is essential: Hubei, China, December 2019 A coronavirus outbreak in Wuhan soon spread to more than 100 countries; in March 2020, WHO declared COVID-19 a pandemic. With a high number of cases and mortality rates, the far-reaching consequences of a global pandemic continue to be a major global agenda item. Throughout the epidemic, communication efforts were ongoing to inform the public, raise awareness, implement preventive measures, and ultimately mitigate the pandemic and prevent the collapse of the country's health care system. The media played an important role in disclosing information to the public and health authorities. Nevertheless, the infodemics spreading from modern communication technologies and social media hindered the dissemination of accurate information. Given the lack of health literacy in Turkey, the rapidly changing and unstable pandemic environment resulted in information gaps and missed information. The importance of media literacy and health literacy, especially in digital media, was reemphasized. This study assesses the impact of risk communication and media on society during the COVID-19 pandemic. It also assesses key concerns about the media during the risk period, including the pandemic. Erdal Ozkaya (2018) is cybersecurity challenges in social media. It has been reported that user data is being sold to third parties and personal data is being accessed for advertising purposes with or without consent. There is also a new wave of security threats, breeding on social media platforms. Social engineering is becoming a formidable security threat due to the volume of data that users post on social media platforms. Hackers do not need to search deeply for data they can use to attack users. Attackers lurking on social media platforms and working hand-in-hand with revenue-driven social media platforms are making it difficult for social media users to continue to enjoy social media platforms in peace. In response, this study investigated the ways in which social media platforms inherently keep users from security and privacy threats. We hypothesized that social media platforms are culprits in increasing the security and privacy threats faced by users and conducted research to prove it. As a result, it was observed that social media platforms have made users more vigilant about their online security. Secondary data sources also revealed that there are many social media users who are exposed to security and privacy risks but are unaware of it. Based on the findings from the primary and secondary data, several recommendations were formulated with the hope of mitigating the security and privacy issues that users face on social media. The recommendations aim to make users more secure, encourage government participation in regulating social media platforms, and give social media platforms more control over user privacy. Faizul Nizam Abu Salim (2019) et al. Strategic Use of Social Media in Risk Communication Social media is a communication platform whose use and influence has grown exponentially in recent years, especially in citizenship journalism The rise of citizenship journalism and 24-hour journalism in particular has democratized the communication process. Risk/crisis communicators can put into practice the principles advocated in good communication practices and make them central to risk management and communication methods. Malaysia's social media penetration rate is 75%, ranking 7th in the world as of January 2018. This "double-edged sword" nature of social media, if approached as an opportunity rather than a challenge, can be successfully leveraged in risk and crisis communication to help improve emergency preparedness and response, reduce disaster costs, improve transparency in decision-making, and increase the likelihood of acceptance of outcomes. First and foremost, it is an excellent listening tool to pick up on risk incidents being discussed in the social media realm as part of the Early Earning Surveillance System (EWARS) and help "feel the pulse" of the public. It helps bridge the polarization and gap between public perception and the perception of authorities/regulators/experts, an important issue that needs to be successfully addressed in risk communication. Communication about risks and crises is valuable in enhancing preparedness and response, as it helps to raise the level of public awareness and increase their ability to take appropriate measures. Identifying effective risk communication strategies to inform both the public and professionals is essential to promote and achieve appropriate patterns of behavior that reduce public health risks, whether emerging diseases, chemical or radiation threats, or familiar annual risks such as haze or flooding. It is essential to Different types of social media and mobile messages can play complementary roles in risk and crisis management. Social networking media can help strengthen coordination among volunteers and emergency services. At the same time, content-sharing media can help implement situational awareness, as many users share

real-time images and videos of how the crisis is developing. We have seen this time and again in Malaysia, especially in relation to major events that are of interest to many and evoke an emotional response from the general public. To share best practices by the Malaysian Ministry of Health on how social media can be used strategically in risk and crisis communication, we use several case study examples of actual incidents: 20, Girish Raja (2023) et al, Research: using data science methods to analyze security issues on social media Social media, as with other media, includes resistance to targeted phishing, protection of business accounts from hacking, prevention of fraud, account hacking such as protection from social engineering scams, and other unique risks. It is difficult to provide social media security for accounts that are associated with a business or that are private. Social media security is the act of analyzing data from recently active social media platforms to help users protect themselves from the consequences. Despite the security settings of social media networks, some with ulterior motives succeed in obtaining extremely important personal information. Data is collected from users and analyzed for future phases using machine learning techniques. Gohar Feroz Khan (2017) et al. address social media risk management in this chapter in Social Media Risk Management. Issues related to identifying, assessing, mitigating, evaluating, and assessing social media risk are discussed. Common social media risks include reputation damage; leakage of confidential information; legal, regulatory, and compliance violations; impersonation and hijacking; loss of intellectual property; viruses; and privacy issues. Techniques for securing social media platforms include two-mode authentication, strong passwords, and third-party applications: in the COVID-19 pandemic planning and response in Turkey, the novel coronavirus infection (COVID-19) declared a global pandemic by the World Health Organization (WHO) on March 11, 2020. Citizens were then required to stay home. During this process, social media became a window to the global village of users. As the quarantine process has been prolonged, the use and importance of these platforms has increased in communication, entertainment, socialization, and access to immediate information about the pandemic. People and institutions responsible for pandemic management have begun to make frequent use of social media platforms in their risk communication activities to raise public awareness about the disease and reinforce individual beliefs in compliance with preventive measures. In this study, we analyzed the Twitter account of the Minister of Health, who is responsible for planning and responding to the COVID-19 pandemic in Turkey. The posts shared by the Minister of Health were content analyzed and the messages communicated to the public were examined in terms of the health belief model: Ding Huiling, Jingwen Zhang Clemson University Abstract: Despite widespread praise for social media's ability to enable public participation in content creation and distribution, institutional and cultural constraints do not automatically guarantee open and transparent communication in not automatically guarantee open and transparent communication. Our research on the use of social media during the H1N1 influenza pandemic in the United States and China indicates that government agencies may use social media tools for unilateral risk decisions and policy dissemination, or for limited two-way risk communication. In contrast, the public can circumvent institutional control of risk information through non-institutional participatory risk communication to learn the truth about emerging risks. [China Media Research. 2010; 6(4): 80-91] Keywords: risk communication, participation, social media, novel influenza, extra-institutional The novel influenza pandemic, in its early stages, has shown the immense potential and In its early stages, the H1N1 influenza pandemic caused tremendous fear around the world, both because of its immense potential and the paralyzing potential for economic loss it might cause. With the development and production of vaccines, fears of a new influenza pandemic have been greatly alleviated. However, the potential for mutation of the avian influenza virus still looms nearby. Because avian influenza is a constant pandemic threat that can occur in any part of the world, studying risk communication practices in both Western and non-Western cultures is necessary for us to collaborate with other cultures in a global epidemic. Previous risk communication research has emphasized the need to move from one-way, linear risk communication to participatory risk communication. Social media tools can help break down linear, one-way risk communication and make it more participatory by making it multi-channel. However, patterns of social media use can vary widely across cultures. This comparative study of risk communication practices in the U.S. and China shows that U.S. healthcare organizations utilize social media tools for real-time risk communication. In China, on the other hand, public health institutions made little use of social media, despite the public's reliance on all forms of social media to obtain risk information. As a comparative study on risk communication through social media, this study not only helps to understand the creation and exchange of user-generated knowledge, but also assesses its impact on risk communication. It also points out gaps and problems in existing risk communication theories and the potential for extending such theories to better address new problems and novel situations. The paper begins with a review of risk communication theories, drawing attention to major issues that have not been well explored, such as cultural differences in various cultural contexts, national interests, and media structures. What follows is an analysis of the different ways in which government agencies, for-profit Internet portals, and communities used social media to communicate risks related to the H1N1 influenza pandemic during the early stages of

the epidemic. Various approaches to using social media for participatory risk communication and their implications for those interested in promoting open two-way communication during health risks will be discussed. Risk Communication and Social Media Risk Communication and Alternative Media Grabill and Simmons (1998) refer to the general linear risk communication model as the "technocratic approach," which refers to risk communication as a They view risk communication as a one-way, linear process in which scientists and experts function as knowledge producers providing risk analysis and the public becomes the consumer of such knowledge. They believe that the technocratic approach is inappropriate because it ignores power relations, audience participation, and democratic decision-making; Leiss and Powell (2004) note that there is a marked difference between "the scientific and statistical language of experts and the intuitively grounded language of the general public." blamed for the lack of success in risk communication. Effective risk communication practice requires "breaking down the barriers between the two languages [of experts and laypeople]" and "facilitating productive interaction between the two domains" (p. 29). One of the problems with existing risk communication theories is that their units of analysis are concentrated in North America. It fails to address the cultural, political, and infrastructural differences between North America and other countries with vastly different political and communication structures, as well as the challenges posed by challenges to traditional risk communication practices: exploratory studies have shown that the use of social media is becoming an essential part of modern society becoming an everyday activity. Excessive and compulsive use of social media can lead to social media addiction (SMA). The main objective of this study is to investigate whether demographic factors (including age and gender), impulsivity, self-esteem, emotions, and attention bias are risk factors associated with SMA. The study was conducted on a non-clinical sample of college students (N=520) between the ages of 16 and 23, consisting of 277 females (53%) and 243 males (47%). All participants completed surveys measuring impulsivity, self-esteem, anxiety, depression, social anxiety, loneliness, and attention bias. The final hierarchical regression model indicated significant risk factors for SMA with 38% accuracy. Associated risk factors identified included femininity (= -0.21, t = -4.88, p<0.001), impulsivity (= 0.34, t = 8.50, p<0.001), self-esteem (= -0. 20, t = -4.38, p<0.001), anxiety (= 0.24, t = 4.43, p<0.001), social anxiety (= 0.25, t = 5.79, p < 0.001), and negative attention bias (= 0.31, t = 8.01, p < 0.001). Finally, we present a discussion of the results and make recommendations for future research: social media is a promising area in disaster research as an emerging data source, We conducted a bibliometric analysis using 1573 relevant articles published in Web of Science between 1991 and 2019. The results show that (1) the annual number of papers and the number of new institutions in this field grew rapidly, but appears to have reached saturation in recent years; (3) research hotspots are evolving along a "conceptualization-improvement-application" pathway; and (4) the number of new research institutions is growing rapidly, but appears to have reached saturation in recent years. Three characteristics of social media data-timeliness, subjectivity, and disequilibrium-still present obstacles to applicable disaster types and population representativeness, These findings point to potential directions for the development and innovation of social media-based disaster research Thorell (2021) et al. found that gaming and social media addiction among college students: associations with gender differences, symptom conformity, and psychosocial difficulties; previous studies have shown that addiction to digital media has a negative impact on psychosocial health. Internet Gaming Disorder (IGD) is the most academically recognized, but the potential negative effects of Social Media Disorder (SMD) have also been found. However, few studies have assessed the symptoms of these two digital media addictions in the same way, making comparisons difficult. This study aims to fill this gap by investigating differences and similarities regarding symptom commonality, gender differences, symptom conformity, and association with psychosocial difficulties. Methods 688 college students (63.2% female, mean age 25.98 years) were asked to complete a questionnaire measuring IGD and SMD symptoms and psychosocial difficulties (e.g., psychosomatic disorders, poor self-concept, social problems). Results Results showed that 1.2% of men and 0.9% of women met the symptom criteria for IGD (no significant difference), while 3.2% of men and 2.8% of women met the symptom criteria for SMD (no significant difference). Dimensional analysis showed that men scored higher on IGD than women, but the opposite was true for SMD. Symptoms of high digital media involvement (i.e., "preoccupation," "tolerance," "withdrawal," "not trying to control well," and "escape") had high sensitivity but low positive predictive value (PPV). However, symptoms associated with negative consequences of digital media use (i.e., loss of interest, continued excessive use, deception, and career/relationship jeopardy) had lower sensitivity but higher PPV. These symptom patterns were similar for IGD and SMD; meeting criteria for IGD or SMD and being at risk for these disorders were significantly associated with psychosocial difficulties; SMD symptoms were generally more strongly associated with psychosomatic illness than IGD symptoms; and PPV was more strongly associated with psychosomatic illness than IGD. Conclusions Involvement in digital media appears to be common not only among patients with IGD or SMD, but also among those who do not meet the symptom criteria; SMD appears to be more common than IGD and is associated equally or more strongly with psychosocial difficulties: the coronavirus (COVID-19) epidemic

has been a major source of disasters in many countries around the world, including The coronavirus (COVID-19) epidemic has caused several disasters in the health and lives of people in many countries around the world. Even though everyone is at risk of infection, regardless of ethnicity, income, age, or political affiliation, the consequences of this epidemic will have a profound impact on the Global South at the level of its very fragile sanitary structures, economic, social, and cultural infrastructure. This study examines the key determinants of the adoption of social media in managing a public health crisis of international concern such as COVID-19 and the impact of its use. We propose a theoretical framework that combines several approaches, including the Health Belief Model, the Technology Acceptance Model, and Social Influence theory. In addition, this study will conduct a variety of surveys using mixed research methods. The findings and recommendations of this study will serve as a research foundation for considerations and strategic actions to be implemented by government agencies, health organizations, and associations to effectively combat COVID-19 and provide effective information to marginalized communities through the use of social media. Khadijah Angawi, Mutlaq Albugmi (2022) et al. Impact of Social Media on Risk Perception during the COVID-19 Outbreak in Saudi Arabia Background Social media is considered an important source for seeking health information, especially during an outbreak. During the Coronavirus Infections 2019 (COVID-19) pandemic, social media played an important role in disseminating information. However, it became a source of misinformation in many areas throughout the pandemic. Whether this disseminated information had a positive or negative impact, individuals' risk perceptions of disease were affected; it is important to explore the factors shaping public behavior and adaptation to risk reduction measures during the COVID-19 pandemic. Therefore, the purpose of this study is to determine the role of social media and its impact on risk perception of COVID-19 in Saudi Arabia. Methods This was a cross-sectional study, and participants were recruited through various social media from August to October 2020. The survey was administered through the Qualtrics platform to Saudi residents aged 18 years and older. The survey was conducted in English and Arabic. Convenience sampling was used to recruit survey participants. Links to the survey were posted on several social media platforms. Results A total of 2,680 respondents completed the online survey. Results indicated that gender was positively and significantly associated with risk perception for males, those with incomes between 4,000 and 12,000 SAR, and those who were employed compared to others (: 0.044, p-value: 0.035, : 0.051, p-value: 0.041, : 0.108 p-value: < 0.001, : 0.119 p-value: < 0.001). In the second block, risk perception was higher for those who were more exposed to social media (: 0.096, p-value: < 0.001). In the third block, self-efficacy was significantly but negatively correlated with risk perception, indicating that those with higher self-efficacy were less likely to perceive risk for COVID-19 (: -0.096, p-value <0.001). There was no interaction between social media and self-efficacy on risk perception. Conclusions The results of this study indicate that social media exposure to COVID-19 information has a positive impact on the formation of individuals' risk perceptions. The study also suggests that public officials and policy makers need to develop effective communication strategies through risk communication campaigns, as women, individuals of lower socioeconomic status, and single individuals showed negative associations with risk perception. Linda R. Wilbanks (2020) et al. Cyber Risk in Social Media Social media is a common Internet tool used by businesses to communicate with customers, clients, vendors, and other businesses. It is also used to conduct financial transactions with customers, pay employees, and manage the company. However, social media and the Internet contain latent risks that companies should be aware of that could affect the company, its employees, and its customers. Companies need to be aware of what social media risks are and what steps they can take to mitigate them. While social media threats cannot be eliminated, actions can be taken to reduce the probability of a threat's success and mitigate the impact if it does succeed. If a given threat gains access to the Internet, a company may fail financially or damage relationships: (2020) et al, Social Media Security Threat Research and Mitigation Methods: a Preliminary Review, in Recent Advances in Data Collection and Combined Statistics, Big Data has become a key issue in a variety of research areas, including: machine learning, data mining, social networking, and artificial intelligence. Social networking is used as a platform for a variety of applications, including government, business, education, politics, dating, and marriage. Like each platform, social networking has its pros and cons. This study will examine the types of postings to social media sites, the impact of posted data, and the privacy concerns of Facebook and Twitter users. The study demonstrates the various user concerns about posting information and the impact of user voiced privacy concerns. Social networking can be beneficial in areas such as education, advertising, and online shopping, but people can become addicted to social networking, spend time on a variety of issues, and be exploited by cyber criminals. We have discussed the purpose of e-government using social media. Social networking is also vulnerable at various stages and can be attacked in several ways including evil twin attacks, virus attacks, phishing attacks, account takeover, data breach attacks, fraud and scams. Site monitoring, security policy development, user education, training programs, software updates, archiving, and media content are some mitigation techniques used to reduce the impact of cyber attacks: the last technological revolution coming space, place, com-

pletely overturned the long-established relationships between communication flows, affecting the way in which information is territorialized and, conversely, the way in which territories are (re)formed in a virtual dimension. In particular, the Internet and the social web have further accelerated the growth of geotagged data co-created by non-expert users. The increased co-creation of space-related information also has implications for risk awareness and disaster management. On the one hand, there has been a significant increase in the flow of disaster-related data disseminated by institutional actors for a wide variety of purposes (disaster management, on-site disaster management, real-time information). On the other hand, a significant amount of data is being co-created and shared by users in a bottom-up fashion by integrating official sources of information while the disaster crisis is still ongoing. This chapter provides a theoretical review and a series of descriptive examples, inserted theoretically at the intersection of communication geography and disaster geography, that illustrate the increasingly pervasive role of ICTs in risk awareness and management. Michael Cross (2014) describes the risks of social media. While everyone has information they want to keep secure, the possibility of sensitive data being leaked is a genuine concern. There is also the risk of affecting trust if the information shared is false. This or other events could result in public embarrassment, loss of reputation, and possibly loss of customers. We will also look at how risks such as loss of data or equipment can be mitigated through the various tools available on the Internet and through the regular process of archiving critical data. Hauer, Suruchi Sood (2020) et al. (2020) argue that effective crisis and risk communication strategies that utilize social media to communicate sustainable preventive measures and reduce misinformation, especially during emergencies such as the SARS-CoV-2 (COVID-19) global pandemic, are extremely important. Social media, with its global reach, is an important source of news and information about COVID-19. However, the flood of misinformation about personal defense measures that people post on social media has created an urgent need for a better understanding of effective messaging strategies. Improving the quality and strategy of information disseminated through social media is critical not only to minimize anxiety and panic and curb misinformation, but also to improve the adoption of sustainable preventive measures. Understanding the components of an effective health communication strategy can help identify common ways to address misinformation and, in turn, help people adopt appropriate preventive measures. The purpose of this article is to understand how effective social media communication strategies can be developed to promote sustainable prevention measures and curb the misinformation that is spread. Health and communication agencies provide information for effective social media messaging and, more importantly, serve as a gateway to other resources. We will review their recommendations to identify common elements of social media communications regarding the adoption of sustainable precautions and effective strategies to curb misinformation. In addition, we examine social media messaging during the Ebola and Zika fever outbreaks to assess the success of social media strategies and draw lessons learned.Mohammad Alaa Hussain Al-Hamami (2015) and others have shown that social media platforms with Security Implications. Due to its importance, social media has become a major target of cyberwar and criminals. Attackers can obtain a lot of valuable information from social media. This chapter describes the security implications in social media and their impact on individuals, businesses, and governments. The chapter also discusses the risks of using the Internet, the importance of social media to attackers, what can go wrong with social media, examples of techniques attackers use, why attackers are successful in their attacks, social media issues from a legal perspective, social media security environment, common security models for social media websites, data that can be mined, points of attack, security defenses against attacks, methods of security attacks, reasons to attack social media, social media programming flaws, Social media security strategies and policies, social media privacy and government, emerging trends in social media security, and social media best practices will also be discussed. Nicole S. Kuhn, Shawon Sarker, Lauren White, Josephine Hui, Serena McCray, and Clarita Hurtand-Begey (2020), et al. Decolonizing Risk Communication: in this exploratory study, American Indian and Alaska Native (AIAN) governments and organizations to examine how they are using social media to share critical health information about coronavirus infection 2019 (COVID-19) with their citizens. Through a thematic analysis of 119 public Facebook posts by tribal governments and organizations, three broad categories and 13 sub-themes were identified. Tribal governments and organizations had created risk communication materials for their respective communities that fell into three categories: (1) risk mitigation, (2) meeting the needs of local residents, and (3) maintaining connections with the community and culture. Our findings indicate that during the COVID-19 pandemic, AIAN communities and organizations played an important role in disseminating credible and culturally adapted risk communications and critical community information to tribal populations through social media. Such communications included clear illustrations, posts, and messages about wearing masks, social distancing, the importance of hand washing, mandatory border closures, and suggestions for staying connected to the community. In doing so, they are filling a gap in ensuring that communities receive the relevant information they need to mitigate and manage risk. In order to understand how to better meet community needs, further efforts are needed to improve the well-being and visibility of

the AIAN population in the areas of health disparities, technology, social media, and the many impacts of COVID-19: COVID-19 in Zanzibar. case study, social media is widely used in health communication promotion, but its online and offline relevance is largely unexamined. This qualitative study explored the role of social media in mitigating COVID-19 infection in Zanzibar and its impact on people's health, using a sample of 30 communication professionals and health professionals. The results revealed that social media is a powerful platform for providing health awareness information to mitigate COVID-19 and that these platforms have enabled people to understand the local medicines used to mitigate COVID-19 infection. Furthermore, there is a high association between online health information and offline people's health behaviors. Furthermore, social media use does not pose a threat to people's health during a pandemic, but there is a high risk of affecting people without Internet media literacy. Although social media does not pose a threat to some users with high levels of Internet media literacy, in order to make these platforms more useful for mitigating infectious diseases without compromising public health in Zanzibar and Africa as a whole, all people should be Digital media literacy should be provided. Unknown authors (2022) et al. in Risk Communication and Social Media, novel coronavirus infection (COVID-19) was declared a global pandemic (pandemic) by the World Health Organization (WHO) on March 11, 2020. Citizens were then required to stay home. During this process, social media became a window into the global village for users. As the quarantine process has been prolonged, the use and importance of these platforms has increased in communication, entertainment, socialization, and access to immediate information about the pandemic. People and institutions responsible for pandemic management have begun to make frequent use of social media platforms in their risk communication activities to raise public awareness about the disease and reinforce individual beliefs in compliance with preventive measures. In this study, we analyzed the Twitter account of the Minister of Health, who is responsible for planning and responding to the COVID-19 pandemic in Turkey. The posts shared by the Minister of Health were content analyzed and the messages communicated to the public were examined in terms of the health belief model. Sarah C. Voss, Janet Sutton, Yue Yu, Scott L. Renshaw, Michele K. Olson, C. Ben Gibson, and Carter T. Butts (2018), Risk Communication Retweets: Social media platforms such as Twitter and Facebook provide risk communicators with the opportunity to quickly deliver messages to constituents in the event of an emerging outbreak. These platforms increase the exposure of the message through message passing (called "sharing" on Facebook and "retweeting" on Twitter). This raises the question of how to optimize risk messages to spread throughout the network and thus increase message exposure. This study adds to this growing body of work by identifying message-level strategies to increase message delivery in highly ambiguous events. In addition, we will use an extended parallel process model to examine how threat and efficacy information affects the delivery of Zika fever risk messages.In August 2016, we collected 1,409 Twitter messages about Zika fever sent from U.S. public health agency accounts. Using content analysis techniques, we identified features inherent in the messages and analyzed the impact of those features, the account that sent the message, the network surrounding that account, and the prominence of Zika fever as a topic using negative binomial regression. The results suggest that severity and efficacy information increase the frequency with which messages are passed on to others. Based on the results of this study, previous research on message delivery and diffusion theory, we identify a framework for risk communication on social media. This framework includes four key variables that influence message delivery and identifies a core set of message strategies, including message timing, that can increase exposure to risk messages on social media during highly ambiguous events. Shiv Arora, Rajesh Kumar, and Kashvi Piplani (2022) et al. Social Media Addiction - Risk of Addiction in India as measured by the Bargaining Social Media Addiction Scale (BSMAS): social media use has increased since its inception in the early 2000s and Social media use has continued to increase since its inception in the early 2000s. While some aspects of behavioral addiction, such as online gaming, have been recognized as addictive, excessive social media use requires more research to validate the same. This study considers aspects of the cognitive-behavioral model theory of general pathological Internet use in its approach to deciphering social media addiction. Objective This study aims to determine what percentage of the population under study is at high risk of developing social media addiction and to analyze the factors prevalent among Indian users. MATERIALS AND METHODS The objectives will be achieved by using the questionnaire-based BSMAS scale, applying exploratory factor analysis to the BSMAS, and validating the tool against Indian social media users. The study focused on India, and 747 respondents were selected through convenience sampling; short and Likert scales of the BSMAS, exploratory and confirmatory factor analysis were applied. RESULTS AND CONCLUSIONS: 18% of the sample were at risk of developing social media addiction; EFA reduced the six factors of the BSMAS to three factors, Salience, Mood Modifications/Tolerance, and Relapse, explaining 37.4% of the total variance. Confirmatory factor analysis validated the scale for the Indian population: sampling validity by Kaiser-Meyer-Olkin's KMO measure was 925, and internal reliability of the data was very good at 89. Bartlett's sphericity test had a chi-square value of 4034.47 /153 with a p-value of less than .001, indicating that the sample is suitable for EFA. Unknown

authors (2023) et al. investigate: analysis of security issues on social media using data science methods Social media, like other media, has a number of security issues, including resistance to targeted phishing, protection against hacking of business accounts, prevention of fraud, account hacking and protection from social engineering scams such as account hacking, and other unique risks. It is difficult to provide social media security for accounts that are associated with a business or that are private. Social media security is the act of analyzing data from recently active social media platforms to help users protect themselves from the consequences. Despite the security settings of social media networks, some with ulterior motives succeed in obtaining extremely important personal information. Data is collected from users and analyzed for future phases using machine learning techniques. Tom Hart, Christopher Brewster, and Duncan Shaw (2012), et al. Crisis Communication and Social Media: Changing Environments in Natural Disaster Response Several major disasters (Haiti earthquake, Australian floods, UK riots, Japan earthquake) have occurred in the past two years and disaster response Social media has been widely used in disaster response, often in innovative ways. This paper analyzes how social media have been used in communication from the public to the public and from the public to government organizations. Four ways in which disaster response has been transformed by social media will be discussed: 1. 1. Social media appear to be replacing traditional media as a means of communicating with the public during crises. In particular, social media is influencing the way traditional media communications are received and delivered; 2. User-generated content is a potential new source of information for emergency management agencies during disasters, but the reliability and usefulness of that information is uncertain; 3. Some point out that social media provides a means for citizens to self-organize in ways that were not previously possible. However, the type and usefulness of self-organization sometimes works against efforts to mitigate the consequences of disasters.4. Social media appears to affect the flow of information during disasters. In the past, most information flowed in one direction, from government organizations to the general public, but social media negates this model. While the general public can easily spread information, they also expect interaction with government organizations rather than a simple one-way flow of information. These changes also affect how government organizations and citizens communicate with each other during disasters. The primary model for describing this form of communication, Crisis and Emergency Risk Communication (CERC), was developed in 2005, before the widespread adoption of social media. We present a modified version of the CERC model that integrates social media into the disaster communication cycle and addresses how social media has changed communication between the public and government organizations during disasters: social media has grown to become an important component of modern life and is having both beneficial and detrimental effects on people's health. Several parents and activists have recently expressed concern about the possible negative effects of social media use. According to some studies, social media use is very likely to result in poor mental health outcomes, including suicide, loneliness, and a significant decrease in empathy. Other studies either did not substantiate a risk or suggested that some people may benefit from social media. Among the consequences of heavy social media use are increased mental illness, panic disorder, and decreased tolerance. Findings from different age groups concluded that social media confers some benefits but is also harmful. However, an imprecise registry revealed lifelong suicidal ideation, indicating that this particular attitude may be a sign of a more serious problem. This study focuses on how social media affects people's lives. Wu He (2013) investigated mobile social media security risks through blog mining and extensive literature search. The purpose of this paper is to survey the latest developments in the security aspects of mobile social media, identify recent trends, and provide recommendations for researchers and practitioners in this rapidly evolving field. Design/methodology/approach - This paper reviews the disparate discussions in the literature on security aspects of mobile social media through blog mining and an extensive literature search. Based on the in-depth review, the authors summarize several key insights to help companies understand the security risks associated with mobile social media. Findings - Based on the findings of the review, the risks associated with mobile social media are identified. Provide best practices and useful tips to help enterprises mitigate mobile social media risks. Also provide insights and guidance to help enterprises mitigate mobile social media security risks.

2.4 Social Risk Management

Previous Research Case Studies (2011) in 'Social Protection Policy for Poverty Reduction in Colombia: Conceptual Challenges' discuss that Ten years after the "war against poverty," the persistence of poverty and vulnerability in the face of financial and environmental crises, as well as the growing inequality of income and resource access, represent the challenges inherited from the 2000-2010 decade in terms of social protection. These challenges are even more significant when one considers that the concept of 'social risk management,' around which the model of social protection on a global scale was articulated over the past decade, was initiated alongside the promise of transforming risk into a socio-political issue, or, in other words, a topic of planning, prevention, and management and no longer a factor related to uncertainty characteristic of an uncertain and interconnected world. The continuing social effects of similar crises at the end of the

1990s represent a call to reexamine the risk management focus of social protection. This article discusses the legacy of Holzmann and Jorgensen's seminal paper from 1999 on 'social risk Fecha de recepción: 26 de febrero de 2010 Fecha de aceptación: 15 de diciembre de 2010 Fecha de modificación: 8 de marzo de 2011 Additionally, Previous Research Case Studies (2016) in 'Social Risk Management Strategies and Health Risk Exposure – Insights and Evidence from Ghana and Malawi' discuss that Risk exposure is a major cause of poverty, deprivation and persistent vulnerability worldwide. This volume analyzes individuals' and households' responses to a variety of risks, with an emphasis on health risks. The study adapts the Social Risk Management (SRM) conceptual framework and extends it considerably for academic inquiry. Using household data from Ghana and Malawi, empirical evidence is provided on the complex relationship between high risk exposure and the application of proactive and reactive SRM strategies (incl. health insurance), showing their specific contributions to risk management. The PhD thesis has been published as monography in the series "Social Protection in Health - Challenges, Needs and Solutions in International Health Care Financing" at LIT-publisher. "Social Protection in Health - Challenges, Needs and Solutions in International Health Care Financing" des LIT-Verlages erschienen. Additionally, Previous Research Case Studies (2016) in 'Social Risk Management as a Strategy in the Fight Against Poverty and Social Exclusion' discuss that Questions surrounding the fight against poverty and social exclusion have become a global priority. Poverty and its causes are perceived as differences in the economic and social development of each individual continent and country. Social risk management was developed by the World Bank as a specific conceptual framework of social protection strategy and includes prevention, mitigation and the management of social risks. The diverging causes of poverty across the European continent assume a different approach in identifying causes and social risk management. An important aspect of the EU's social policy is to combat unemployment and social exclusion with the support of the European fund to help the extreme poor and other EU funds, e.g. EQUAL. The appropriate implementation of social risk management in each country is a prerequisite for reducing extreme poverty. Social risk management as a global strategy to combat poverty and extreme poverty is a challenge in the field of education which offers a new range of views and is generating more complex professional competencies in education and new possibilities for university graduates in the labor market. Additionally, Previous Research Case Studies (2021) in 'Social Risk Management as a Response to Increasing International Pressure for Social Performance' discuss that In the past decades, financial institutions have led the way for companies to adhere to international standards for social performance. The journey began in the Industrial Revolution, when negative societal business impacts rapidly escalated, which led people to demand for their management. Initially focused on working conditions, impacts on the environment soon started to gain notice. Halfway through the 20th century, a combination of oil spills and mass media attention generated enough public pressure for the United States to sign the first piece of legislation requiring the environmental impact assessment. With this law and its replication abroad, however, came the concern with social impacts as well. Both environmental and social performance expectations soon spread internationally and, by the 1980s, multilateral financial institutions, most prominently the World Bank, incorporated such considerations into their investment and lending practices, which is the source of all such international standards today. These standards require the establishment of a social management system to integrate risk and impact management processes and stakeholder engagement activities. Given the challenge of implementing these requirements, a social risk management development framework is proposed to bring together the extensive and multidisciplinary demands of effective social performance. Five development areas are proposed: governance, social policy, tools, resourcing and capacity, and knowledge sharing. This is an important step to take today as it is expected that the next decades will see these international demands increase, possibly by ever increasing governmental regulation. Additionally, Previous Research Case Studies (2014) in 'Social risk management' discuss that A method includes a protected social entity is determined based on one or more user inputs, and data on one or more social networks that is related to the protected social entity is monitored. A risk to the protected social entity is determined based on monitoring the data on the one or more social networks that is related to the protected social entity. The risk management data is provided to a user. Additionally, Previous Research Case Studies(2010) in 'Social risk management system and method' discuss that The present invention provides a social risk management system and method capable of analyzing data pertaining to an economic venture, identifying social risks that may be encountered, generating specific prevention and mitigation measures for those hazards, and evaluating the results. In one embodiment, the present invention provides a user-friendly graphic user interface through which users may access the unique functionality of the present invention. In one embodiment, the present invention is capable of utilizing feedback data to generate one or more evaluation reports illustrating the success, or lack thereof, of the implemented prevention/mitigation measures. Additionally, Previous Research Case Studies (1987) in 'Social Risk Management' discuss that The risk problems facing society today have many characteristics that limit and otherwise complicate the application of formal analysis. Since not all prob-

lems possess these complicating qualities to the same degree, some problems may be addressed more effectively by certain decision-aiding approaches than by others. To identify the most useful approach, the analyst must clearly understand the decision problem being addressed. A comparative evaluation of approaches must therefore begin with a characterization of social risk management decisions. Additionally, Previous Research Case Studies (2020) in 'Implementation of government programs of social risk management' discuss that Introduction. Accelerated pace of development of society contributes to the accelerated generation of social risks, modern society is characterized by constant technological, natural, economic, environmental, socio-cultural changes. Therefore, minimizing social risks and leveling their consequences is of paramount importance.Methods. Diagnosis of the state of the social risk management system combined the principles of systemic, structural-functional and targeted analysis, which provided a comprehensive assessment of the whole and individual components.Results. The analysis of expenditures on the social sphere showed their stable absolute growth despite the dynamic reduction of their share in the budget. Social risks are largely due to the non-transparency of the mechanism for regulating the supply and demand of labor in the domestic labor market. A significant share of macroeconomic social risks is related to the problems of social infrastructure, which is financed from the budget. Problems with access to health care, the opacity of the pharmaceutical market, the degradation of the health care network, chronic underfunding, and the lack of health insurance also generate social risks. The task of state policy should be to prevent and prevent social risks, identify social conflicts that lead to destructive consequences. Systematization of social risks allows to methodologically substantiate the mechanisms of social risk management, to modernize the models of social protection of the population, to develop effective tools for ensuring public management of social risks.Discussion. The impossibility of reducing funding for social needs without deteriorating the quality of life and social protection of the population requires further search for alternative sources of funding for socio-cultural expenditures, rationalization in the budget structure to effectively combat the development of social risks. Additionally, Previous Research Case Studies (2014) in 'Social Risk Management on german labour market' discuss that Terms such as social policy and labor market policies seem not be actual more. Instead, we speak more and more about risk management. Social Risk Management is a concept developed by the Word Bank. It is a tool to transfer management techniques from the operating or finance in the social and labor market policy, to support individuals, households and communities to better manage their risk. Due to poor incentive structures, inadequate insurance policies or control often remain under preventive, palliative and solidarity balancing risk management measures. This paper sets out to define the term of social risk management, describing the basic features from different perspectives and the main measures and strategies used in social risk management area. The essay considers the most discussed word of risk management as a moral opportunity to redefine the balance of responsibility and solidarity in the labor market. Additionally, Previous Research Case Studies (2000) in 'Social risk management :a new conceptual framework for social protection and beyond' discuss that This paper proposes a new definition, and conceptual framework for social protection, grounded in social risk management. The concept repositions the traditional areas of social protection (labor market intervention, social insurance, and social safety nets) in a framework that includes three strategies to deal with risk (prevention, mitigation, and coping), three levels of formality of risk management (informal, market-based, public), and, many actors (individuals, households, communities, non-governmental organizations, governments at various levels, and international organizations) against the background of asymmetric information, and different types of risk. This expanded view of social protection emphasizes the double role of risk management instruments - protecting basic livelihood, as well as promoting risk taking. It focuses specifically on the poor, since they are the most vulnerable to risk, and typically lack appropriate risk management instruments, which constrains them from engaging in riskier, but also higher return activities, and hence gradually moving out of chronic poverty. Additionally, Previous Research Case Studies(2001) in 'Social Risk Management A New Conceptual Framework for Social Protection, and Beyond' discuss that This paper proposes a new definition and conceptual framework for Social Protection grounded in Social Risk Management. The concept repositions the traditional areas of Social Protection (labor market intervention, social insurance and social safety nets) in a framework that includes three strategies to deal with risk (prevention, mitigation and coping), three levels of formality of risk management (informal, market-based, public) and many actors (individuals, households, communities, NGOs, governments at various levels and international organizations) against the background of asymmetric information and different types of risk. This expanded view of Social Protection emphasizes the double role of risk management instruments?protecting basic livelihood as well as promoting risk taking. It focuses specifically on the poor since they are the most vulnerable to risk and typically lack appropriate risk management instruments, which constrains them from engaging in riskier but also higher return activities and hence gradually moving out of chronic poverty. Additionally, Previous Research Case Studies(2003) in 'Social Risk Management: The World Bank's Approach to Social Protection in a Globalizing World' discuss that Social protection is moving up on the development agenda. Dismissed as ineffective, expensive

or even detrimental to development in developing countries for a long time, it is now increasingly understood that assisting individuals, households and communities in dealing with diverse risks is needed for accelerated poverty reduction, and sustained economic and social development. Conceptually, social protection is shifting towards social risk management to reduce the economic vulnerability of households with appropriate instruments and to help them smooth consumption patterns. For the poor countries, it is about moving away from unproductive coping strategies adopted by households (such as removing children from schools, delaying health care, selling livestock) that are buffeted by shocks (such as drought, cyclones, floods, conflict, terms of trade, policy reforms, health, unemployment, etc.). It seeks to replace these strategies with ex-ante planning and mechanisms to help households anticipate and insure against these shocks (through public works, weather-based insurance, water management, grain storage, micro-savings, etc.). For all countries, it is about rethinking the design and implementation of traditional public interventions such as labor market, social insurance, and social assistance policies. The paper outlines the development aspect of social protection, presents the social risk management concept and its operationalization in risk and vulnerability assessments, explains the focus on vulnerable groups (such as children and the disabled), and briefly reviews traditional programs such as labor market interventions and pensions through the social risk management lens. Additionally, Previous Research Case Studies(2007) in 'The Role of Social Risk Management in Development: A World Bank View — Reply to Comments' discuss that 1 SRM as a conceptual framework Social risk management is a conceptual framework about the importance of risk and of risk management instruments for poverty reduction and development. The proposed conceptualisation emphasises risk (including uncertainty) that can be easily translated into a loss of income (also human capital, and by extension other important outcomes), and stresses the key strategies and arrangements for dealing with risk. SRM undoubtedly has a bias toward economic interpretation and much of our SRM work in the Bank is in this vein. But as a framework, SRM is open to alternative specifications. In our view, much or all of what has been proposed in the comments can be accommodated within the framework. Which of the complementary or alternative specifications (or hypotheses) should be introduced and selected is in the end – as in any science – an empirical question. Additionally, Previous Research Case Studies (2002) in 'Social Risk Management: A Conceptual Fallacy of Composition' discuss that The World Bank is developing a new conceptual framework for social protection. Designed to be more appropriate than conventional contributory social security for meeting the multitude of labour market and non-labour market risks faced by the chronic poor in developing countries, this conceptual framework is called 'social risk management' (SRM). A critical analysis of the SRM framework is presented, with the aim of sharing with risk practitioners and academics alike some important insights into this recent and largely unreported development in social policy. The article concludes on a somewhat critical note by stating that, although there remains a recognised need to improve mechanisms of social protection for the poor in developing countries, the SRM framework appears not only to be conceptually flawed from the perspective of risk theory, but also inherently limited in its ability to fulfil its key policy aim of poverty alleviation through the better management of risk. Additionally, Previous Research Case Studies (2019) in 'Social Protection in an Era of Increasing Uncertainty and Disruption : Social Risk Management 2.0' discuss that This paper updates the Social Risk Management (SRM) conceptual framework; the foundation of the World Bank's first Social Protection Sector Strategy. SRM 2.0 addresses the increasingly risky and uncertain world; with opportunities and outcomes driven by possible disruptions from technology, markets, climate change, etc. SRM 2.0 is a spatial assets and livelihoods approach to household well-being featuring a risk chain covering all households across the lifecycle and for both positive and negative events. Key findings: Location and context are critical for household choices; assets are key to sustainable resilience to poverty, new assets and livelihoods need to be considered for the 21st century, and resilience and vulnerability to poverty are two sides of the same coin. Operationally, SRM 2.0 points to the need for a greater focus on asset and livelihood building programs in addition to traditional poverty alleviation and risk sharing programs, better integration between rights-based and risk-based approaches, more inclusive targeting, and consideration of global social protection.

3. Discussion

3.1 Application of immune networks to provide autonomous accident avoidance capabilities for automobiles.

Consider the idea of applying the evaluation of self-organizing traffic accident avoidance systems using immune networks. While systems that utilize the biological problem-solving mechanisms of immune networks to provide vehicles with autonomous accident avoidance capabilities and other systems are in practical use Consider adapting this concept to risk information management systems in society. First, the network algorithms used for autonomous decentralized accident avoidance need to be reconstructed and models devised for application to the detection, evaluation, and management of various social risks. This includes risk detection in social risk management (similar to accident detection in automobiles), response mechanisms (similar to avoidance behavior), and cooperative risk management strategies (similar to coop-

erative vehicle selection), etc. Immune network models can be applied to facilitate dynamic and adaptive responses to evolving risks in society The following are some of the most important To propose a mathematical model of a risk information management system in society, one could adapt the key concepts of the traffic accident avoidance system in this paper based on the immune network approach used in this paper. In this paper, we first considered the following Risk Detection Function (RDF) Similar to the accident detection mechanism in automobiles, this function evaluates the probability of various risks in society. It uses parameters such as frequency, severity, and historical data to construct indicators of risk Risk Response Mechanism (RRM) Similar to avoidance behavior in transportation systems, this mechanism determines the best response to identified risks. It involves parameters such as response time, effectiveness, and resource allocation. Coordinated Risk Management (CRM) Reflecting a collaborative vehicle selection mechanism, this aspect involves a coordinated effort among various social actors (governments, organizations, and communities) to manage risks. Parameters include level of cooperation, communication efficiency, and shared resources.

These functions are interlinked in a dynamic self-organizing network that adapts to changing social conditions and risks, much as an immune network adapts to new pathogens. This represents a model of an autonomous decentralized accident avoidance system based on immune network theory. To adapt these equations to a society's risk information management system, we can reinterpret them as follows

The equation dAi(t)/dt can represent the rate of change over time of awareness of a particular risk in a population. ai(t) is the activation level of the risk management response, similar to the activation of an immune response. dri(t)/dt can be used to model the change in risk level due to control measures. Ri(t) can represent the probability of a crisis if the risk is not properly managed.

Parameters need to be adjusted to the social context, such as defining what constitutes an interaction between risks and what is implied by the risk level and the corresponding level.

3.2 Detailed societal risk information management system based on the immune network model

Also, to propose detailed mathematical formulations and parameters for a societal risk information management system based on the immune network model, you could consider the following adaptations:

For the risk influence factor $r_i(t)$, you might define it based on societal metrics such as economic impact, health impact, social unrest potential, etc.

The differential equation for the risk level $dr_i(t)/dt$ could include terms that represent the rate of risk spread, the rate of mitigation due to management actions, and the natural decay of the risk over time. The response function $R_i(t)$ could be based on the logistic function as shown, but the parameters might be adjusted to reflect how quickly society can respond to the risk once it's recognized. Link weights T_{ij} could be adapted to reflect the influence or correlation between different risks or between different societal responses. Utility function U_i could measure the effectiveness of the response to risk i, with parameters tuned to reflect the importance of different types of risks or responses.

These equations would need to be calibrated with real-world data to ensure that they accurately reflect the dynamics of societal risk management. The calibration process would involve statistical analysis and possibly machine learning techniques to fit the model parameters to observed outcomes of risk management efforts.

More, To summarize and adapt the equations from traffic model to a societal risk information management system:

1. Change in Risk Awareness (dAi/dt):

$$\frac{dA_i(t)}{dt} = \sum_{j=1}^{N} m_{ij} a_j(t) - \sum_{k=1}^{M} m_{ik} a_k(t) + m_i - k_i a_i(t)$$

Where $A_i(t)$ is the awareness of risk i at time t, m_{ij} and m_{ik} are the influence factors of other risks and responses on risk i, and m_i, k_i are the inherent growth and mitigation rates for risk i.

2. Risk Response Activation (ai):

$$a_i(t) = \frac{1}{1 + \exp(ran - A_i(t))}$$

Here, $a_i(t)$ represents the activation level of the societal response to risk i at time t, modulated by the risk awareness $A_i(t)$.

These equations can help model the dynamics of risk awareness and management in society, capturing how different risks and management strategies influence each other over time. The parameters m_{ij}, m_{ik}, m_i, and k_i would be determined based on empirical data of societal risks and their interactions.

In the equations provided, the terms are defined as follows:

i: Index representing a specific risk within the system.
N: The total number of risks that can influence a given risk i.
M: The total number of management responses or strategies that can influence risk i.

In the context of a societal risk information management system, N would encompass all the different risks being monitored, while M would represent the various response mechanisms or strategies in place to manage those risks. Each risk i is influenced by other risks and management strategies, affecting the overall awareness and response activation levels in the society.

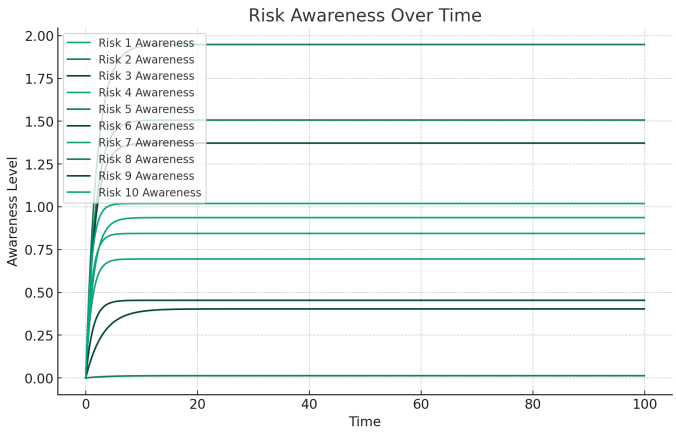

Fig. 4: Risk Awareness Over Time for ten different risks

From the graph provided, which depicts Risk Awareness Over Time for ten different risks, we can infer certain dynamics about the risks labeled as "Risk 1 Awareness" through "Risk 10 Awareness." Particularly, we can focus on risks that could be interpreted as 'impersonation risk' (potential for identity fraud or masquerading) and 'conflict of opinion risk' (potential for disagreements or disputes due to differing views).

Here are some observations and considerations based on the graph and the provided simulation equations:

From Steady State Awareness, All risks seem to reach a steady state relatively quickly. This implies that awareness of these risks is becoming constant over time, which could suggest that the society has acknowledged the risks and is continually mindful of them. And Rapid Initial Increase, The steep initial slope for all risks indicates a rapid increase in awareness after the risks are identified. This could reflect an effective dissemination of information about the risks or a strong initial reaction to their identification. Impersonation Risk, If we consider one of the risks to represent 'impersonation risk', the graph shows that awareness of this risk stabilizes at a high level. This could imply that once the awareness of impersonation risks is raised, it remains high, potentially due to ongoing media attention, regular occurrences reminding people of the risk, or effective continuous education. Opinion Conflict Risk, Similarly, if another risk represents 'conflict of opinion risk', the graph suggests that awareness is also maintained at a high level. This could be interpreted to mean that society is consistently aware of the potential for conflict arising from differing opinions, which may be due to the pervasive nature of such conflicts in social interactions and public discourse.

Regarding the simulation equations, they suggest the following dynamics:

Influence Factors ($m_i j$ and $m_i k$) These factors determine how much one risk's awareness affects another and how management responses affect risk awareness. In the context of impersonation and opinion conflict risks, these factors could represent how public awareness campaigns or news reports about one risk can influence the awareness of the other.

Inherent Growth and Mitigation Rates (m_i and k_i) These rates are intrinsic to each risk and reflect how naturally the risk awareness grows or is mitigated over time without external influences. For risks like impersonation, a high inherent growth rate might be expected due to the increasing prevalence of online interactions. For opinion conflicts, the inherent rate might be influenced by the current political climate or cultural attitudes towards debate and discourse.

Risk Response Activation (a_i) The activation level of societal response is a function of awareness and represents how prepared or responsive society is to a particular risk. The sigmoid function suggests that there is a threshold effect: once awareness reaches a certain point, the societal response becomes significantly more activated.

In summary, the graph and the equations together imply a society that quickly becomes aware of risks and then maintains a consistent level of awareness, potentially due to a combination of factors including media coverage, public discourse, and inherent societal dynamics. Both impersonation risk and opinion conflict risk appear to be well-recognized within this society, with sustained awareness that could enable ongoing management and mitigation efforts.

4. Conclusion

From here, we will further conclude the discussion of this paper with the idea of adding a component that allows the system to autonomously adjust the influence factor between risk and response to the idea of an autonomous decentralized emphasis avoidance network algorithm. This is similar to how a vehicle in a traffic model adjusts its own behavior based on the behavior of neighboring vehicles.

4.1 Ecentralized emphasis avoidance network algorithm into the model

To incorporate the idea of an autonomous, decentralized emphasis avoidance network algorithm into the model, we can add components that would allow the system to autonomously adjust the influence factors between risks and responses based on the current state of the system. This would be similar to how vehicles in the traffic model would adjust their behavior based on the behavior of neighboring vehicles. Here's an idea for an additional component to the model:

Decentralized Emphasis Adjustment (dmi/dt): - The influence factors m_{ij} and m_{ik} could be dynamic, changing over time based on the success or failure of the current risk responses. - Introduce a new term $dmi_{ij}(t)/dt$ and $dmi_{ik}(t)/dt$ which represents the rate of change of influence factors over time.

The new differential equations might look like this:

$$\frac{dmi_{ij}(t)}{dt} = f_{ij}(a_i(t), a_j(t), \Delta A)$$

$$\frac{dmi_{ik}(t)}{dt} = f_{ik}(a_i(t), a_k(t), \Delta A)$$

Where f_{ij} and f_{ik} are functions that determine how the influence factors change based on the activation levels of the risks and the changes in risk awareness (ΔA).

These functions f_{ij} and f_{ik} could be designed to increase the influence factors when a risk is not being adequately managed (as indicated by an increasing $A_i(t)$) and decrease them when the current strategies are effective. This would allow the network to self-organize and "learn" over time which strategies are most effective for managing different risks, similar to how an immune system learns to deploy the most effective responses to pathogens it has encountered before.

Implementing this idea requires setting up additional rules for the adjustment functions f_{ij} and f_{ik}, which might involve complex adaptive systems concepts such as reinforcement learning or other bio-inspired algorithms that can adapt based on historical performance data.

Incorporating stability control elements into the autonomous decentralized network algorithm for societal risk management could be conceptualized by adding feedback mechanisms that adjust the influence factors based on the deviation of the system from a desired stable state. This approach would be akin to control theory, where the system self-regulates to maintain equilibrium.

Here's an idea for incorporating stability control into the model: Stability Control for Decentralized Network (dmi/dt with feedback) Implement a feedback loop that adjusts the influence factors based on the error between the current state and a target stable state. The rate of change of influence factors over time could now also depend on this error term, which measures how far the current risk levels are from the desired levels. The modified differential equations might include an error term $e_i(t)$ and look like this:

$$\frac{dmi_{ij}(t)}{dt} = g_{ij}(e_i(t), a_i(t), a_j(t))$$

$$\frac{dmi_{ik}(t)}{dt} = g_{ik}(e_i(t), a_i(t), a_k(t))$$

Where: - $e_i(t) = A_{target} - A_i(t)$ represents the error for risk i at time t, with A_{target} being the target awareness level for risk i. - g_{ij} and g_{ik} are new functions that adjust the influence factors based on the error term as well as the activation levels of risks and management strategies. These new functions g_{ij} and g_{ik} could be designed such that when the error $e_i(t)$ is positive (i.e., the risk awareness is below the target), the system increases the influence factors to boost the response. Conversely, if $e_i(t)$ is negative (the risk awareness exceeds the target), the system would decrease the influence factors to prevent overreaction and maintain stability. Additionally, to prevent oscillations or over-adjustments, you might introduce a damping factor into the adjustment functions to smooth the transitions. This is similar to a PID (Proportional-Integral-Derivative) controller in control systems, which often includes terms to adjust for the present error (P), the accumulation of past errors (I), and the prediction of future errors (D).

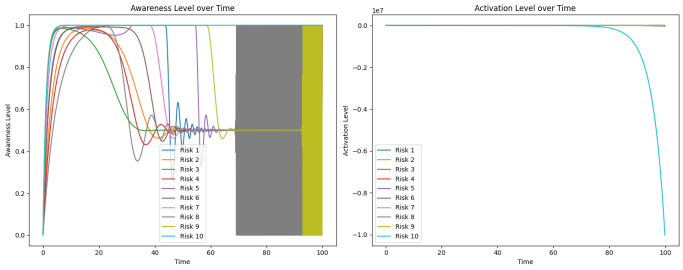

Fig. 5: Activation Level over Time Graph / Awareness Level over Time Graph

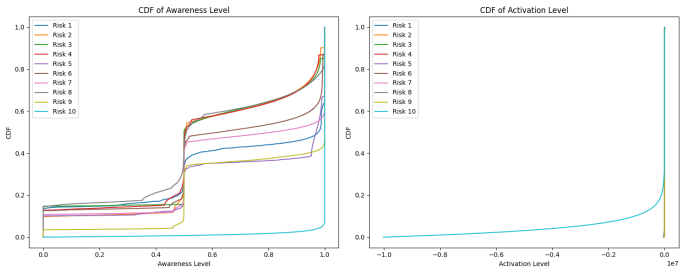

Fig. 6: CDF of Awareness and Activation Levels

Implementing stability control elements would help the system to not only learn and adapt to managing risks based on historical data but also to maintain a desired state of risk awareness and response activation, leading to a more robust and stable risk management network.

Analyzing the new set, we can gain insights into the dynamics of risk awareness and activation levels over time, which can help us understand the nature of impersonation risk (like identity theft or fraud) and opinion conflict risk (such as social or political disputes).

4.2 Awareness Level over Time Graph

Peaks and Valleys**: Different risks experience peaks in awareness followed by declines. This suggests a fluctuating interest or concern over these risks, which could be due to new information, events, or shifts in public attention.

Stabilization

Post-peak, most risks seem to stabilize at a certain level of awareness, though some fluctuate widely (Risks 1, 2, 3, 6, and 9). This could indicate ongoing discussions or events

that keep these risks in the public eye, preventing a consistent level of awareness.

Gray Zone

There is a shaded area on the graph that may represent a period of uncertainty, data unavailability, or a critical event that affects all risks. The awareness for most risks drops sharply here, suggesting a possible collective shift in attention or a disruptive event that causes a loss of focus on these specific risks.

Activation Level over Time Graph

This graph depicts how the societal response to risks is activated over time. Observations:

Immediate Response

There is a quick activation for all risks, implying a rapid response once awareness reaches a certain threshold.

Long-Term Activation

After the initial response, activation levels plateau, indicating sustained action or mitigation strategies against these risks.

CDF of Awareness and Activation Levels

These graphs show the cumulative distribution function (CDF) of both awareness and activation levels, which helps to understand the probability distribution of these metrics over time.

4.3 CDF of Awareness

The distribution suggests that for most risks, awareness levels are bunched at the higher end of the scale, indicating that most of the time, awareness levels are high.

4.4 CDF of Activation

The CDF for activation shows a skewed distribution, with activation levels clustered at the extreme end. This could mean that once the activation level for a response reaches a certain point, it is likely to stay high.

Implications for Impersonation and Opinion Conflict Risks

If we associate certain risks with impersonation and opinion conflicts, we can infer:

Impersonation Risk

This risk likely sees spikes in awareness due to specific events (such as data breaches). The societal response seems to be robust, as indicated by the activation level plateauing. However, the fluctuations in awareness suggest that maintaining consistent attention to this risk may be challenging.

Opinion Conflict Risk

Awareness of this risk might be more stable unless specific events trigger fluctuations. The activation response seems to be strong, suggesting that once society recognizes the need for managing opinion conflicts, measures are put in place and maintained.

Autonomous, Decentralized Emphasis Avoidance Network Algorithm

The idea of incorporating an autonomous, decentralized emphasis avoidance network algorithm into the model is advanced. It suggests the model can adapt the influence factors dynamically, akin to an immune system that adjusts its response to pathogens over time. If applied to risks like impersonation and opinion conflict, this could mean the societal response becomes more tailored and effective as the system "learns" from past experiences. In essence, the system is designed to self-optimize, potentially leading to more effective management of risks as time progresses. This could be particularly useful for impersonation risk, where strategies may need to evolve quickly in response to new threats, and for opinion conflict risk, where the effectiveness of conflict resolution strategies could improve with experience.

The overall analysis of these graphs and the proposed model modifications indicates a complex interplay between risk awareness, societal response, and the ability of the system to adapt over time. It points to a society that is not static in its risk responses but one that could potentially learn and improve its risk management strategies over time.

4.5 'Velocity' at which the risk state Network Algorithm

Here is a conceptual translation of that algorithm into the risk management context: The algorithm provided related to calculating the Time to Collision which is a measure commonly used in traffic systems to assess the danger or risk associated with the current distance and relative velocity of vehicles. we would adapt the concept to reflect the 'distance' (or difference) between the current state of a risk and a target state, and the 'velocity' at which the risk state is changing.

1. Define a "Time to Target State" analogous to TTC, which measures the time it would take for the current risk level to reach the target risk level, assuming current trends continue. 2. The TTS could be used as part of the error term in your stability control functions g_{ij} and g_{ik}, influencing the rate of change of the influence factors.

$$e_i(t) = A_{target} - A_i(t)$$

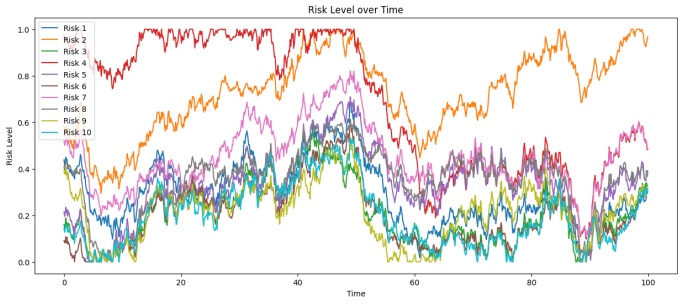

Fig. 7: Risk Level over Time

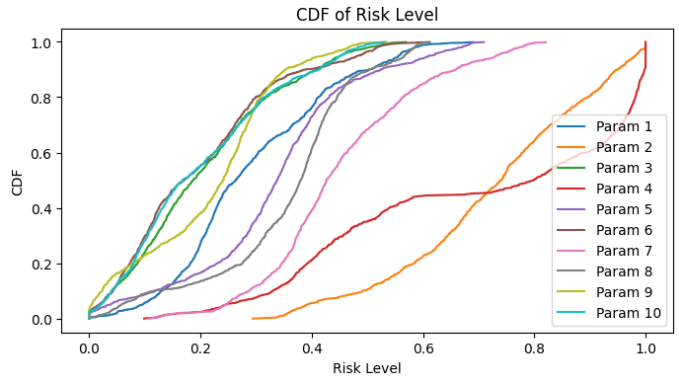

Fig. 8: CDF of Risk Level

(Error term representing the deviation from the target state)

$$TTS_{ij} = \frac{e_i(t)}{\frac{dA_i(t)}{dt}}$$

(Assuming $\frac{dA_i(t)}{dt}$ is not zero)

$$\frac{dmi_{ij}(t)}{dt} = g_{ij}(TTS_{ij}, a_i(t), a_j(t))$$

$$\frac{dmi_{ik}(t)}{dt} = g_{ik}(TTS_{ik}, a_i(t), a_k(t))$$

Where g_{ij} and g_{ik} could be designed to adjust the influence factors based on , and potentially include a damping factor to smooth transitions and prevent system oscillations.

The graphs depict the evolution of risk levels over time and the cumulative distribution function (CDF) of both influence factors and risk levels. Using these, we can examine the dynamics of risks such as impersonation (spoofing), opinion conflict, social distancing, and response velocity.

Risk Level over Time Graph

Variability

he graph shows significant variability in risk levels over time, suggesting that the risks are influenced by various fluctuating factors. For example, impersonation risk might fluctuate due to varying attack techniques or awareness campaigns, while opinion conflict risk could vary with political or social events.

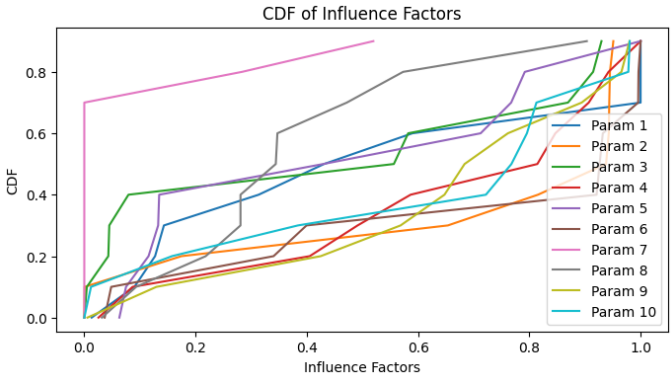

Fig. 9: CDF of Influence Factors

Trends

Certain risks (like Risk 1 and Risk 2) show an overall increasing trend, indicating that these issues are becoming more prominent over time. If Risk 1 represents impersonation, it suggests an increasing problem, potentially exacerbated by technological advances.

Convergence and Divergence

Risks appear to converge and diverge at different points in time. This could represent the interaction between different societal factors or events that either align the perception of risks or cause them to be viewed more individually.

CDF of Influence Factors Graph

Distribution

The CDF of influence factors indicates that some parameters (such as Param 1 and Param 10) have a higher likelihood of having greater influence, which might reflect factors such as media coverage or policy changes that significantly affect risk perception.

Influence Heterogeneity

The spread between the curves suggests that the influence factors for risks are diverse, meaning that not all risks are influenced equally by external factors. This could affect the speed and effectiveness of societal response to these risks.

CDF of Risk Level Graph

Risk Exposure

The CDF of risk levels shows how often certain risk levels are reached or exceeded. A steep curve for a risk suggests that high risk levels are less common, whereas a more gradual curve (like for Param 1) indicates that high risk levels are more frequent.

Long-Tail Risks

Some risks have long-tail distributions, meaning that while they often maintain a moderate level, they occasionally spike to very high levels. This could be critical for risks like impersonation or opinion conflicts, indicating that while usually managed, there are times when these risks become acute.

Overall, the analysis of the graphs and the simulation framework suggests that managing these risks involves understanding both the current state and the velocity of change, as well as the influence factors that drive these changes. The goal is to maintain risk levels within acceptable bounds, reacting appropriately to trends, and preventing over- or under-reaction to fluctuations in the risk landscape.

Impersonation Risk

If one of these risks represents impersonation, such as identity theft or spoofing, it could be the one with significant spikes and troughs. This might indicate that events such as data breaches or new phishing techniques cause sudden increases in risk, while successful interventions or awareness campaigns might reduce it temporarily.

Opinion Conflict Risk

This could be associated with the risk that shows periodic peaks, possibly correlating with external events such as elections or social movements. It could also be a risk that has a consistent baseline with occasional spikes, indicating a persistent underlying issue that flares up in certain conditions.

Social Distancing

If the context is related to health risks, a line that shows cyclical behavior might correspond to social distancing. Peaks could indicate times when social distancing measures are lessened and troughs when measures are increased or adhered to more strictly.

Response Velocity

The speed at which the risk level changes could indicate response velocity. A risk with sharp ascents and descents might suggest quick responses, whereas more gradual slopes could indicate slower societal or institutional responses.

Influence Distribution

This graph shows how frequently certain influence factors are at different levels. If influence factors represent public attention or regulatory measures, then curves closer to the top-right might indicate more consistent or stronger influences on risk management.

Risk Distribution

This CDF shows the distribution of risk levels over time. A curve that rises quickly to the top might indicate a risk that is often low but has the potential to spike (long-tail risk). Conversely, a curve that is more gradual suggests a risk that is more uniformly distributed across levels.

The "Risk Level over Time" graph could be used to calculate the derivative $\frac{dA_i(t)}{dt}$, which represents the velocity of risk change.

The "CDF of Influence Factors" graph helps understand the distribution of the influence factors, which could be used to adjust the parameters m_{ij} and m_{ik} in the simulation equations dynamically.

The "CDF of Risk Level" graph would be instrumental in setting the A_{target} within the error term $e_i(t)$ and determining the Time to Target State TTS_{ij} and TTS_{ik}.

By combining these graphical insights with the simulation equations, one could model the dynamic response to risks, aiming to keep the risk levels within desired bounds and adjusting the influence factors to effectively manage the risk profiles over time. This might be particularly useful for creating policies and responses that are both proactive and reactive to the changing nature of these risks.

Aknowlegement

The author is grateful for discussion with Prof. Serge Galam and Prof.Akira Ishii.

References

zh

[1] Sîrbu, A., Loreto, V., Servedio, V.D.P., & Tria, F. (2017). Opinion Dynamics: Models, Extensions and External Effects. In Loreto V. et al. (eds) Participatory Sensing, Opinions and Collective Awareness. *Understanding Complex Systems*. Springer, Cham.

[2] Deffuant, G., Neau, D., Amblard, F., & Weisbuch, G. (2000). Mixing Beliefs among Interacting Agents. *Advances in Complex Systems*, **3**, 87-98.

[3] Weisbuch, G., Deffuant, G., Amblard, F., & Nadal, J. P. (2002). Meet, Discuss and Segregate!. *Complexity*, **7**(3), 55-63.

[4] Hegselmann, R., & Krause, U. (2002). Opinion Dynamics and Bounded Confidence Models, Analysis, and Simulation. *Journal of Artificial Society and Social Simulation*, **5**, 1-33.

[5] Ishii, A. & Kawahata, Y. (2018). Opinion Dynamics Theory for Analysis of Consensus Formation and Division of Opinion on the Internet. In: Proceedings of The 22nd Asia Pacific Symposium on Intelligent and Evolutionary Systems, 71-76, arXiv:1812.11845 [physics.soc-ph].

[6] Ishii, A. (2019). Opinion Dynamics Theory Considering Trust and Suspicion in Human Relations. In: Morais D., Carreras A., de Almeida A., Vetschera R. (eds) Group Decision and Negotiation: Behavior, Models,

and Support. GDN 2019. Lecture Notes in Business Information Processing 351, Springer, Cham 193-204.

[7] Ishii, A. & Kawahata, Y. (2019). Opinion dynamics theory considering interpersonal relationship of trust and distrust and media effects. In: The 33rd Annual Conference of the Japanese Society for Artificial Intelligence 33. JSAI2019 2F3-OS-5a-05.

[8] Agarwal, A., Xie, B., Vovsha, I., Rambow, O. & Passonneau, R. (2011). Sentiment analysis of twitter data. In: Proceedings of the workshop on languages in social media. Association for Computational Linguistics 30-38.

[9] Siersdorfer, S., Chelaru, S. & Nejdl, W. (2010). How useful are your comments?: analyzing and predicting youtube comments and comment ratings. In: Proceedings of the 19th international conference on World wide web. 891-900.

[10] Wilson, T., Wiebe, J., & Hoffmann, P. (2005). Recognizing contextual polarity in phrase-level sentiment analysis. In: Proceedings of the conference on human language technology and empirical methods in natural language processing 347-354.

[11] Sasahara, H., Chen, W., Peng, H., Ciampaglia, G. L., Flammini, A. & Menczer, F. (2020). On the Inevitability of Online Echo Chambers. arXiv: 1905.03919v2.

[12] Ishii, A.; Kawahata, Y. (2018). Opinion Dynamics Theory for Analysis of Consensus Formation and Division of Opinion on the Internet. In Proceedings of The 22nd Asia Pacific Symposium on Intelligent and Evolutionary Systems (IES2018), 71-76; arXiv:1812.11845 [physics.soc-ph].

[13] Ishii, A. (2019). Opinion Dynamics Theory Considering Trust and Suspicion in Human Relations. In Group Decision and Negotiation: Behavior, Models, and Support. GDN 2019. Lecture Notes in Business Information Processing, Morais, D.; Carreras, A.; de Almeida, A.; Vetschera, R. (eds).

[14] Ishii, A.; Kawahata, Y. (2019). Opinion dynamics theory considering interpersonal relationship of trust and distrust and media effects. In The 33rd Annual Conference of the Japanese Society for Artificial Intelligence, JSAI2019 2F3-OS-5a-05.

[15] Okano, N.; Ishii, A. (2019). Isolated, untrusted people in society and charismatic person using opinion dynamics. In Proceedings of ABCSS2019 in Web Intelligence 2019, 1-6.

[16] Ishii, A.; Kawahata, Y. (2019). New Opinion dynamics theory considering interpersonal relationship of both trust and distrust. In Proceedings of ABCSS2019 in Web Intelligence 2019, 43-50.

[17] Okano, N.; Ishii, A. (2019). Sociophysics approach of simulation of charismatic person and distrusted people in society using opinion dynamics. In Proceedings of the 23rd Asia-Pacific Symposium on Intelligent and Evolutionary Systems, 238-252.

[18] Ishii, A, and Nozomi, O. (2021). Sociophysics approach of simulation of mass media effects in society using new opinion dynamics. In Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 3. Springer International Publishing.

[19] Ishii, A.; Kawahata, Y. (2020). Theory of opinion distribution in human relations where trust and distrust mixed. In Czarnowski, I., et al. (eds.), Intelligent Decision Technologies, Smart Innovation, Systems and Technologies 193.

[20] Ishii, A.; Okano, N.; Nishikawa, M. (2021). Social Simulation of Intergroup Conflicts Using a New Model of Opinion Dynamics. *Front. Phys.*, **9**:640925. doi: 10.3389/fphy.2021.640925.

[21] Ishii, A.; Yomura, I.; Okano, N. (2020). Opinion Dynamics Including both Trust and Distrust in Human Relation for Various Network Structure. In The Proceeding of TAAI 2020, in press.

[22] Fujii, M.; Ishii, A. (2020). The simulation of diffusion of innovations using new opinion dynamics. In The 2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology, in press.

[23] Ishii, A, Okano, N. (2021). Social Simulation of a Divided Society Using Opinion Dynamics. In Proceedings of the 2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (in press).

[24] Ishii, A., & Okano, N. (2021). Sociophysics Approach of Simulation of Mass Media Effects in Society Using New Opinion Dynamics. In Intelligent Systems and Applications (Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 3), pp. 13-28. Springer.

[25] Okano, N. & Ishii, A. (2021). Opinion dynamics on a dual network of neighbor relations and society as a whole using the Trust-Distrust model. In Springer Nature - Book Series: Transactions on Computational Science & Computational Intelligence (The 23rd International Conference on Artificial Intelligence (ICAI'21)).