Human-Centric Cyber Threat Intelligence for Autonomous Vehicle Networks

By Dr. Jing Li

Professor of Electrical Engineering, Tsinghua University, China

1. Introduction

As the rise in interest in the application of integrated autonomous capabilities to Commercial Autonomous Vehicles (CAVs), e.g., robots mobile drones, and especially, Private Autonomous Vehicles, such as autonomous trucks, autonomous trains, and autonomous passenger vehicles, known as autonomous vehicles (AVs), has reached unprecedented levels, we have noted the increasing importance of intelligent security and privacy architectures, ranging from strategies to promote clean-slate techniques to ensure robustness, security, and privacy of AVs. However, many of these security and privacy concerns are far from solved. Furthermore, as ubiquitous AI technologies appear, new challenges must be addressed and not just near term concerns. Although the capability to perceive the environment and to act on this understanding represents a major technological leap, it fails to solve the privacy concerns linked with always-on sensors, or the security threats posed by adversarial challenges to the vehicle's AI at design, test, or operation stages, as well as during handover or back-transition stages.

It is quite clear that AI technologies are revolutionizing the way autonomous driving systems perceive the world and act in response to this understanding. However, it is equally apparent that AI is incapable of tackling many of the major security and privacy issues raised by autonomous driving systems, mainly because AI's core is a learning algorithm, not a security tool. This paper discusses AI's limitations, as well as the security and privacy challenges specific to autonomous driving systems and proposes an approach to address them, which is built upon a new concept that we call Human-Centric Cyber Threat Intelligence. Our approach is agnostic to AI and is complementary to existing autonomous driving systems.

Our proposed architecture supports CAV's autonomous driving capabilities by enabling cheaper, scalable cyber threat data analytics using HCCyTI derived algorithms designed for cross-domain and multi-level CAV security intelligence.

1.1. Background and Significance

For the vehicle, one strategy instantly utilizes sensors and their measuring properties to minimize the duration of connectivity to the cyber network environment. The second strategy employs offline optimized anomaly detection methods, minimizing potential privacy and cybersecurity threats in cyber network environments to ensure safe, reliable, and effective data communication between autonomous vehicle (AV) servers and vehicles. In comparison with anomaly detection methods designed for non-transportation industry network performance, the performance of these models was shown to eliminate "computation hungry" feature metrics such as non-real-time feature interactions, sub-linear time complexity, and iterate during online real-time learning. Among the performance records, social learning and high tolerance to illegally injected adversarial malicious data reduced. For the server-side processing framework, the system directly integrates primitive vehicle-defined subtasks into operational server processing.

Since 2013, several high-profile security violations involving remote car-hacking incidents have drawn attention from car manufacturers, cybersecurity vendors, and government regulators to secure autonomous vehicle networks. Although individual companies have implemented theoretical findings designed for a conventional network environment into commercially viable cybersecurity services, none of these commercial offerings effectively mitigate the cybersecurity vulnerabilities of autonomous vehicle networks. Their work focuses mainly on using cyber threat information to detect and mitigate potential security threats. Instead of using existing cybersecurity services based on unrelated industrial network safety applications, researchers proposed insights describing the reasoning process of vehicle computing and network servers by using closed-loop environmental information.

1.2. Research Objectives

The third scientific challenge aims to uncover the introspection-building blocks for preempting and detecting human role-blind interactions. These interactions occur when humans are exposers of vehicle-cyberspace probing attacks. The goal is to facilitate the

sentinel (risk aversion)-based networked resource allocation and trust architecture. This architecture is essential for achieving adversarial vehicle-cyber resilience.

The second scientific question explores how human and vehicle proximity detection metrics can enhance bandwagon-like information cascading paradigms. These enhancements will enable vehicle mesh networks to reach and predict collective adversarial decisions among adversarial coalitions and independent adversaries.

The first scientific question addresses how to integrate a bounded rational model of autonomous vehicle decentralized communications, interactions, and networked decision making. This integration will be done through a holistic framework that anticipates, engineers, and assesses VCTI failures. The focus is on human-in-the-loop trust and privacy preservation.

The central aim of this research is to develop methods, meta-models, and models for resizing a human-centric network. This network will be able to receive, encode, detect, analyze, compute, predict, and visualize the probability of adversarial vehicle-cyber interactions. These capabilities are crucial for building resilient connected and autonomous systems. This broad objective is guided by three scientific challenges.

As our vehicular infrastructure undergoes a massive transformation, the mobility and trust of vehicle users and stakeholders become critically important. Unfortunately, as vehicles become more interconnected and the safety and convenience systems become more concentrated in the electronic domain, attacks against automobiles will become more commonplace. To fully realize the potential of autonomous systems, it is necessary to scrutinize the unintentional vulnerabilities and explicit risks in the interactions between bounded rational humans and deviant adversaries. This scrutiny must be done with personalized and continuous cyber threat intelligence.

To overcome the challenges associated with connected and autonomous vehicles (CAV) ecosystems, a human-centric network architecture inspired by symbiotic human-vehicle systems has been conceived. In this architecture, vehicle-cyber threat intelligence (VCTI) plays a paramount role. VCTI refers to an autonomous vehicle's capabilities to harness, secure, compute, predict, act, and learn from the cyber threat intelligence embedded in its ecosystem.

By utilizing the extracted information cues, the vehicle can make better-informed threat response decisions.

1.3. Scope and Limitations

Despite the benefits and prospects of AI, SHAI, and ML in CTI, they have several limitations. Without real-time threat report streaming, the incumbent deep learning models cannot be trained or unsupervised to recognize changes, which makes the detection of subtle attacks or APTs difficult. Further, domain experts may find it challenging to understand the training process and thus may lack confidence in the trained model. In addition, it is too laborious and costly for domain experts to classify more than one million rows of records assigned to the "other" domain field. We propose to use semi-supervised learning to place these records into smaller clusters with at least one CONFIDENTIAL keyword, as it will save at least 70% of the domain effort which can be labeled by a domain expert.

As for the data format, domain experts prefer to receive incident data wrapped in two formats, STIX and MISP; both are recommended standards for CTI format. We propose a unified framework to relate domain features with threat reports in various formats.

Our study focuses on utilizing human-centric cyber threat intelligence (CTI) data to train and validate deep learning models for key component extraction, relevance classification, and confidential concern identification in autonomous vehicle networks. We demonstrate the importance of human domain knowledge in extracting relevance and identifying potential confidential concerns. We only consider domain experts with high-level clearance and relevant cyber expertise for real case analysis.

2. Autonomous Vehicle Networks: An Overview

Modeling the vehicle network needs to consider not only the participating entities but also the connection relations between intelligent vehicles, so meeting the need of the era of human-centric cyber-physical systems. In other words, human-centric message delivery based on physical channels of autonomous vehicle networks can be carried out. In the context of intelligent vehicle networks, cyber threat intelligence is increasingly displaying the potential to address the ever-growing queries and concerns from vehicle manufacturers and service providers. Research into intelligence and analytics will not only explicitly recognize cyber

threat intelligence as different from conventional cybersecurity but also demonstrate the distinction when applying it in the smart vehicle context.

In the next era of the intelligent world, the combination of transportation mode and automatic driving technology has attracted the attention of society. For example, autonomous driving (AD) and connected vehicle (CV) networks have appeared or are beginning to play a major role in transportation services. Autonomous vehicle networks refer to vehicle networks in which vehicle-to-anything (V2X) and vehicle-to-vehicle (V2V) communications are used to coordinate the behavior of autonomous vehicles. The network design for autonomous driving technology not only gives rise to new challenges but also exploits many new solutions. The problems can be addressed in real scenarios of smart cities, and the availability of expected results points to current cutting-edge techniques. There are many techniques needing to be improved, such as the prediction of behavior decisions, edge network computing, in-vehicle computing, cloud computing, 5G network deployment, etc. The process of automated decision making involves real-time decisions based on relevant information from factories, vehicles, passengers, and road infrastructures under constraints of time window and costly resources, so providing the ability to better alert entities to relevant dynamics over time.

2.1 Introduction

2.1. Key Components of Autonomous Vehicle Networks

Such networks make the vehicles smarter and aware of surrounding conditions, even if they are not equipped with sufficient sensor capability, especially in cutoff conditions. By sharing the data with all networked vehicles, the general area's situation can be understood. This shared vision concept plays an important role in autonomous vehicles. When a human driver operates a vehicle, the human makes decisions based on current conditions within a visual range, and the architecture to facilitate these intelligent decisions is deployed in the complex brain. The role of the environment in facilitating and reducing the human driver's cognitive load while driving is indispensable. When applying the analogous model from the perspective of autonomous vehicles, load-sharing drone(s) or a remote station will play a role with high-performance computing capabilities to help autonomous vehicles.

Several key components used for data collection and transmission include LiDAR, cameras, inertial measurement units (IMU), GPS, speedometer, radar, and light detection and ranging (LiDAR). The following are key components used to transform data into actionable

information: a data lake to store cues' features, a knowledge base to capture domain knowledge from human experts, predictive models for intent recognition, a context-aware reasoning system (CARS) to reason about the presence of the traffic intent, and a user interface to communicate with the external environment and network. Furthermore, the road infrastructure and other vehicles send vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) messages, respectively, using the Dedicated Short-Range Communications (DSRC) in the IEEE 802.11p frequency band.

2.2. Challenges and Vulnerabilities

Over the last several years, researchers have revealed the vulnerabilities of AVs due to the malicious manipulation of the components commonly found in the sensors or even the AI that processes sensor data. Few research works investigate the challenges, vulnerabilities, and attacks presented by integrating AVs into the mobile ecosystem, let alone respect the user's privacy from the perspective of AV users. The following is a discussion of the vulnerabilities: loss of GPS services; Many idea attacks can cause position errors that deny or revoke GPS services. Attacks on LIDAR and GPS sensors may fool an AV by detecting virtual obstacles. Attacks on GPS services allow hackers to make an AV behave in the correct manner. The induction valve for users is a percentage of tear allergies and is caused by a variety of attacks. The control speed of the tears and other vehicles on the road can be very dangerous. Installing AVs in an environment that lacks privacy sensor techniques, home comfort, and a positive vehicle detection rate is another concern for autonomous vehicle users.

Various technologies have been developed with the promise of advancing and promoting autonomous vehicles (AVs). However, these advanced technologies expose AVs to potential cybersecurity threats. The migration of autonomous vehicles from research to the real world has raised significant security concerns. Hackers exploiting the vulnerabilities of an AV can cause physical injury, death, or great financial loss. There are several reasons why the security challenges surrounding AVs are more complicated: (1) highly complex software: many companies that aim to create autonomous driving systems design, launch, monitor, and update the software; (2) merged software and equipment: software is often closely linked to a chip or sensor that generally involves many different providers; (3) numerous potential components for attack: many complex features could allow for different kinds of cyber-attacks, hence making the job for hackers easier; (4) untested software; (5) an interconnected network; and (6) no clear regulations.

3. Cyber Threat Intelligence in Autonomous Vehicle Networks

The rapid development of connected AVNs (autonomous vehicle networks) will certainly enrich people's lives, but at the same time, it will bring many new cyber threats. For example, Admiral Stavridis described the ultimate weapon in the next war, if war is coming, as being able to little bit of a code that effectively hacks into enemy. In this study, Autonomous Vehicle Networks (AVNs) are regarded as a special use case of IoT networks. The aim of autonomous vehicles (AVs) is to minimize the number of accident-causing behavior, and they permit the driver to hand over the responsibility of controlling the vehicle to the vehicle itself. AVNs generally consist of four main components, including the surrounding environment, the control system, the perception and cognition systems, and the support software and data system. The perception and cognition system deals with the vehicles' ability to observe their environment and understand how to safely operate within it in terms of short-term precision and long-term predictability.

The goal of CTI (cyber threat intelligence) is to provide knowledge about the tactics and procedures of threat actors, and the threats relevant to an organization, helping network security personnel recognize and defeat cyber adversaries. CTIs can be classified into the following three types: strategic, operational, and tactical. In the near future, CTIs transition from a manual research methodology to an automatic, machine learning/analysis-driven approach, ultimately creating dynamic defense and autonomous response mechanisms. Moreover, 5G-based V2X communication (also referred to as vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-everything) enable vehicles to communicate not only with each other, but also with the surrounding environment. This changes the classification of the threat attributes, which obstructs the security enhancement of road transportation by connecting the cyber threat intelligence and V2X communication in AVNs. Hence, a CTI framework is designed for integrating situational awareness methodologies and the effects of cyber threats onto the V2X communication channels, threat actors, platforms, and data flows.

3.1. Traditional Cyber Threat Intelligence

Both humans and computers easily understand the STIX expression through labels (e.g., observation, specimen, expression), values, and attribute language (e.g., pattern, suspicion). These features of STIX representations are suitable for handling traffic intelligence because traffic analysis is initiated during a security situation and operates entirely within the cyber-world, requiring minimal human intervention. However, intelligence is not perfectly

automated because data is not sufficient; the result is determined by rules for experts that provide knowledge such as handling or interpretation. STIX and TAXII, which manage traffic intelligence, use the TAXII services to automatically deliver specific threat intelligence data to different companies or organizations. With growing international standards and security standards, the effectiveness of traffic analysis will also be increasingly exploited in the coming years.

The TCP/IP protocol stack is a central component of the internet and a common foundation of networks and communication within the cyber-world. In addition, cyber-attacks exploiting vulnerabilities in its components can be detected through traffic analysis such as protocol analysis, port and service analysis, and signature-based attack detection. Though traffic analysis is dynamic in that it relies on an operational network, specific contextual data that makes it possible, called traffic intelligence, can be shared using existing intelligence sharing standards such as STIX and TAXII. TCP/IP-based traffic intelligence and traffic analysis are the most representative "traditional" cyber intelligence and analysis methods in the cyber-world because they rely on traffic and address traffic captured during actual operations.

3.2. Challenges in Applying CTI to Autonomous Vehicle Networks

2. Heterogeneous Data Analysis: CTI adopts analysis methods from big data and cloud computing, including data mining, Natural Language Processing (NLP), machine learning, and AI to process the data. These methods search and query vast amounts of data—structured, semi-structured, and unstructured security information—identifying the patterns, trends, correlations, anomalies, and ultimately attributing causality to very advanced and sophisticated threat actors and their campaigns. However, the early works of CTI are based on computer security, especially computer networks, with an emphasis on scientific and cyber-physical attacks. They did not consider the consequences of merging a large number of embedded systems, networks, remote data centers, and databases during vehicle driving. The use of AI and machine learning in automotive networks is an urgent, necessary, and evolving challenge that must be met. Human factors must be taken into consideration at every point of decision-making and include human-like intelligence, bias, error, and belief during autonomous vehicle network communications.

1. Diverse Cyber-Risks: Autonomous vehicle networks are designed with a human-centric approach, encompassing disparate ecosystems, stakeholders, companies, and technologies

that must interface within and beyond the vehicle. The integration of new technologies such as lidar, radar, and V2X systems expands the attack surface of autonomous vehicle networks. Both cybersecurity and safety issues need to be addressed to realize autonomous vehicles. This includes systematic identification, classification, proliferation, mitigation, and resilience planning of their unique automotive cybersecurity protocols, anomalies, and attacks.

As the automotive industry looks to deploy increasingly autonomous vehicles based on cyber-physical systems, stakeholders in automotive cybersecurity must adopt more efficient, effective, and reliable cyber threat intelligence. There is a growing body of literature on cyber threat intelligence (CTI). Past research and practice help the automotive community learn new approaches. Applying CTI in the autonomous vehicle networks presents several challenges:

4. Human-Centric Approach to Cyber Threat Intelligence

In this paper, we wish to explore the creation of a cyber threat intelligence (CTI) engine that takes together the diverse set of data and generates cyber-physical (CP) patterns of interest, which can be of great interest to defending safety and security of autonomous vehicle networks. However, the problem is not as straightforward and cadillacing as in traditional communication networks - given the transition towards autonomous vehicle networks, it is expected that the traffic sources driving the network will have an attribute shift, which necessitates an exhaustive understanding of the end-to-end vehicle technology stack at play, in addition to the communication-based transportation-related knowledge. The domain knowledge of human experts competent in the different parts of the stack is of critical importance. By leveraging human-centric values, many uncertainty metrics associated with the protection of human values can influence automated CTI engines and be of help in providing additional value when guiding the decision-making process of the autonomous vehicle.

The application of cyber threat intelligence (CTI) in the realm of autonomous vehicle safety and security relies on the classification, management, and analysis of cyber-physical patterns of attacks as well as system operation, during which domain experts play a key role. The analysis requires both technical knowledge of the underlying autonomous vehicle technology stack, such as hardware and software that are present at each of the layers and across the state space, as well as a detailed understanding of the traffic that traverses vehicle myriads of interconnection links. Generating such CTI manifest and curating the presented knowledge

repository assumes the form of creating, substantiating, enhancing, and analyzing a formal knowledge graph, whose vertex types represent the entities that are of interest to the CTI domain (the event of threat; and the people and the assets that they are concerned with, such as the vehicle); and whose edge types represent the (direct/indirect) human-generated and machine-observed interactions among the graph's aforementioned vertex types.

4.1. The Role of Human Factors in Cybersecurity

To conclude, there is a discussion about what is still unknown about the topic and provides directions for future research as related to the human, organizational, and economic aspect of security.

A comprehensive study of the hacking environment is presented, including hackers and hacking competitions, motivation for hacking, and their techniques, as well as important regulatory, economic, and organizational issues related to system security. The most comprehensive studies of employee deviance and cybercrime, which incorporate research on both traditional criminology and other scientific disciplines, are also included in the analysis. Security improvements and suggestions regarding employee awareness of and response to the corporate security policy, used tools and techniques for reducing the threats associated with the use of personal devices in the workplace, and corporate culture priorities for enhancing enterprise security are also discussed.

This section focuses on the study of human factors in cybersecurity and presents distinguishing characteristics of non-malicious software (benign software) developers and malicious hackers, such as the existence of motivations, behaviors, communications, and cultural aspects for each group of actors. Understanding the motivations of hackers and benign software developers allows for consideration of the human, organizational, and economic aspects of cybersecurity research.

Although cybersecurity traditionally places a particular emphasis on interactions between hardware, software, data, and networks, the human element is ever present and, in fact, often plays a critical role in cyber-attacks and in determining their impact. This is especially pertinent in the context of autonomous vehicle networks where human benefits, such as greater mobility, are very much dependent on complex human/botnet interactions during vehicle control, safety, and access to location-based and congestion management services.

4.2. Benefits of Human-Centric CTI in Autonomous Vehicle Networks

Through human-centric information generation, sharing, and use, CTI can be used within the CAV scenario, overcoming vehicle owner and user data privacy issues. A CTI system predominantly collects information surrounding adversarial activity, helps respond to security incidents, and assists in identifying weaknesses in computer and network security. Verified CTI can also support the decision process of vehicle infrastructure and relay security products for the purpose of complete CAV protection. With data privacy being a primary concern and often an obstacle in acquiring relevant vehicle-related network and vehicle-internal communication data, this research leverages human-centric sources as an alternative to traditional communication-based CTI. We argue that leveraging elements encompassing human-centric information fundamentally contributes towards CAV CTI development and sharing, respecting privacy aspects, providing enhanced data checks, allowing for strategic derailing measures, and contributing towards the determination of new CAV security products. Such specifics encompass a focus on vehicle user behavior and routine, and reliable information are often leveraged as part of automated decision-making.

We propose human-centric cyber threat intelligence (HC-CTI) to generate threat intelligence from human-centric sources to support more secure and privacy-conscious connected autonomous vehicles (CAVs). We show that autonomous vehicle networks can benefit from HC-CTI. Securing CAVs involves the protection of the data flows occurring within the vehicle, the control data being wirelessly broadcasted, and the broader environment including the roadside contact points as well as the backend infrastructure. An additional requirement is the protection of the privacy of vehicle owners and users with respect to their identities as well as detected information about their behavior patterns. A defined system providing the relevant information to ensure these requirements is cyber threat intelligence (CTI). This encompasses the process of acquiring, analyzing, and sharing generated CTI. Current CTI collections are mainly based on victim data, malware analysis, and network traffic analysis, providing communication-based CTI. We argue that these data sources can only partially be used in the context of CAVs due to their data privacy vulnerabilities and propose human-centric CTI sources as an alternative due to their non-obtrusive nature and thus absence of CAV owner and user privacy issues.

5. Methodologies for Developing Human-Centric CTI

This paper presents a preliminary study of methodologies and tools for developing human-centric cyber threat intelligence for autonomous vehicle networks. Our methodologies take into account the context of application in order to produce intelligence that accommodates human-related aspects at a particular conceptual resolution. We first conduct a threat landscape analysis on the automotive domain to identify the potential threats that a user might encounter when interacting with an autonomous vehicle network (say, the private network of an autonomous vehicle). These threats are then incorporated as part of a human-centric penetration testing scenario, where techniques from adversarial emulation and attack life cycle methodologies are adapted to account for contextual considerations. The methods are summarized neatly along with our preliminary considerations during a hands-on investigation. Finally, we propose a threat intelligence validation methodology to assess the efficacy and applicability of human-centric cyber threat intelligence in the autonomous vehicle space.

This section starts by describing the "Threat Landscape Analysis Methodology" (TAM) for assessing the potential of a threat presented to an automotive context. At testing the threat intelligence produced, by reviewing its capabilities across a set of cautionary scenarios, the validation of the threat intelligence is presented. We also present the methodology in which both challenges are achieved by the Human-centric penetration methodology. We have presented the human investigation in terms of an embodied threat so that they present danger in future scenarios at the same level of abstraction where most cyber punishment is discussed for approaching other methodological works in cybersecurity adversary emulation and attack life cycle, but with contemporary methods for adversarial emulation and attack life cycle. Yet, the interaction with a vehicle scenario rather than the fully generic scenario is presented when it tries to attack the underlying network of vehicles in a set of hands-on experiments.

5.1. Data Collection and Analysis Techniques

Based on the forecasting intelligence and networking services, we collect vehicle traffic, wireless communication traffic, and geo-location data from live testing and data capstone projects, including vehicle communication (VPNs, V2X, vehicular cell and link capabilities), network and sensor transmission handoffs (through coordinated community storage), human alertness and driver precautions, user alerts and sensor detection of sensors, battery, power, and data collection digital signatures collected from the user. Furthermore, general human-

generated broadcast, awareness, feedback, data-store id and data description, storage location, and the principles of communication across mobile phone, tablet, and other devices. The connected V2V and V2X network data is encrypted at the application layer and protected from side-channel and other diagnostic or forensic manifest vulnerabilities.

There are various data collection and analysis techniques used to develop the federated tenant networks such as network and traffic data, user and vehicle application data, human-consent user and community data, and social connector generated data analysis. Sensing data encompasses network traffic structure, including electromagnetic spectrum waves and power, and attached or standalone monitoring devices.

5.2. Machine Learning and AI in CTI

In this world of the internet where free analysis models are not free, due to the additional cost, it becomes a burden for smaller organizations. However, this research proposes a clustering network as a solution, optimizer, and partition the model into multiple parts and assign each organization a particular part. In other words, since the corporations are getting access to the model for free, a fee to converse back is not imposed.

Other than detection, AI is also used for modeling cyber threats. Nunez-Diaz A., Bialy M., and Klein M. (2018), in their work, proposed a conditional Gamma mixture model for Cyber Threat Intelligence. The model is a single-layer architecture model. The research primarily is an attempt to improve traditional statistical models.

A unique way of using AI models in organizations was proposed by Toshki M., Hamasuke T., and Nakachi Y. (2017). An AI-driven alert reduction program was developed that automatically reduced the number of attacks based on the priority, without overlooking the significant ones. As a result, the organization was successful in reducing the number of alerts, which led to a significant reduction in OPEX.

Earth D. and Shuha E. (2015), in their work, have proposed a Multi-Layer Detect Network, whose task is to generate a deep model to detect the spoof attack. The system monitors the traffic data and the spoofing attacks get detected using a Two-Stage Radial Based Function Neural Network (TSRBFNN). If the minimal threshold is met, the data is categorized as belonging to an attack. They emphasize a Filtering Layer that reduces the number of features from the data before the models go through the Network Structure.

It is worth mentioning that AI technologies, like neural networks, have a similar abstraction as a brain. CTI analytics is primarily targeted towards data analytics. AI and Machine Learning can add value in multiple aspects such as recognizing network patterns or classifying malicious anomalies.

6. Case Studies and Applications

Our increasing reliance on vehicle communications and connected infrastructures brings vehicles into a larger cyberspace. Network-enabled vehicles can bring accidents if unaware of threats that may impact vehicle passengers and Internet-connected individuals. Most interestingly, attacks needing both cyberspace and the physical world will potentially lead to unexpected consequences. Automotive safety relies on having up-to-date knowledge to advance defense against evolving cyber threats caused from a borderless medium. The concern and question then is where could the scope of cyber threat intelligence be analyzed and understood to secure vehicles, or even further, to cope with other human-centric risks?

The focus of this chapter is how to establish human-centric cyber threat intelligence (HCTI) for transnational networks. We investigated how to combine the ViCA model with network science, explained human-centric measurements, and offered the concept of a human-centric attack surface. We provided the matrix to rank individuals of the environment space for a better understanding of who will be contacted, collaborated with, or attacked. The concept of insider threat was introduced. A comprehensive review of existing theories was provided in the risk area regarding the TSB's exposure to the attacker and intentionally causing human error. This chapter shall be interesting for cybersecurity and privacy researchers, communication and risk management scholars, and cybersecurity professionals.

6.1. Real-World Examples of Human-Centric CTI in Autonomous Vehicle Networks

The collection phase is complete, and we expect other researchers and the industry to weigh in to ensure the collected CTI is accurate, comprehensive, and timely. This means that this nontechnical problem can significantly influence the skills and effort exerted in the technical problem areas in order to build a complete autonomous vehicle network. Further, we have architected this research so that our application of the human-centric CTI framework is transparent and repeatable. By doing so, we hope to provide guidance to researchers who are new to CTI and encourage the CTI researchers to extend their focus on adversarial human behavior. Our research choices have reflected our assessment of the needs of AI in

autonomous vehicle networks frequently acting upon faulty classifications of humans, communication with other humans and the physical context.

In an effort to extend this groundbreaking intersection, we have provided an application of the Human-Centric Cyber Threat Intelligence framework. We used this framework and its five processes: 1) collection, 2) integration, 3) analysis, 4) production, and 5) dissemination on CTI related to non-malicious insider threats to the autonomous vehicle network. Understanding how humans might be perceived by an AI in autonomous vehicles is error-prone, which requires designers to build AI systems that take into account the error-proneness of human behavior. As we have claimed that CTI in autonomous vehicle networks must be human-centric, we have provided an application of this framework using a nontechnical problem that is a part of our framework that requires technical solutions.

7. Ethical and Legal Implications

It is the informational capabilities of CAVs, often given in the form of ADAS, that provide the value and encourage use. However, the data used and generated in the provisioning of these capabilities may bring with them unwelcome and negative consequences if not treated with sensitivity. Hastening easy use of this data without recognizing its potential threat to explore the boundaries of ethically acceptable operation is a public policy problem of fundamentally "unanticipated consequences." The privacy of individuals, corporate privacy, insurance, law enforcement, security services, security itself, and even additionally people's health, well-being, mental state, attitudes to higher-risk activities and addictions all come to the fore in a hyper-connected world. Undervaluing the potential for damaging side effects may lead to future suffering. Countering those side effects by applying over-strict boundaries may lead to other positive outcomes not being realized. At stake is the tendency for CAVs to be primarily associated with reductionist benefits, both personal and societal, rather than carrying with them a strong ethical framework that supports products' use as well as protecting against abuse.

The security discussion around CAVs (Connected and Autonomous Vehicle networks) revolves around the need to protect the safety and privacy of passengers, even though such conversations tend to view crashes and hangs as the vulnerabilities that need to be most closely protected. The perception of security exclusively in terms of safety focuses the risk discourse around CAVs within traditional transportation policy and also distracts from other

pertinent considerations of such communications-oriented transport. In fact, it is the use of the communications layer within CAVs that makes the potential offerings of CAVs novel when compared to traditional transport. More than the transport of goods or passengers from one point of intent to another, it is the data that is transmitted and generated within CAVs, some of it very personal and private to those involved, that makes the activities now associated with Connected and Autonomous Vehicle networks distinct.

7.1. Privacy Concerns

The spread of potential data leaks on intelligent roadways and vehicle data will spark more privacy mechanisms with stronger designs to keep personal data closely located within vehicles and road-side units. In this chapter, we have tried to capture the basics of how privacy concerns are exercised in the infrastructure — we have scaled down to scenario 2 above. This is described in a few sections above for illustration purposes. Our hope is that after reading this chapter, readers can leverage more preferences on privacy requirements for their vehicles and understand what has been built-in and can be enhanced.

The built-in intelligence for vehicular systems to autonomously operate on specialized algorithms has grown exponentially. Cybersecurity, privacy, and resilience of vehicular systems that embed unique identifiers for vehicles and the data they capture are of major importance. Some degree of trackability due to unique identifiers travels forward to data, hence an analysis of potential vulnerabilities from data being exposed to intelligent public roads is presented in this chapter. We discuss research in IoT for vehicular communications and an intelligent infrastructure to secure this environment. The end result, however, is the privacy designs that have been built-in to protect the data end-to-end. Device behavior and subsequent analytics have gone through a digital forensic process so that the "essence of the device at the time of data extraction" is achieved.

7.2. Regulatory Frameworks

Both governments and international economic organizations are increasingly developing roadmaps for the deployment of connected and autonomous vehicles worldwide. In the case of the European Union, many directives call for the highest standards of safety. The General Data Protection Regulation (GDPR) has driven a global trend of directing oversight on data, which has had an impact on data supply chains (including in the AV context). Finally, our approach aims to register an industry/regulator statement for the generation, management,

and transfer of data, with respect to relevant communities or regulatory frameworks in light of the threats detected by the intelligent sensor system to the ecosystems. The increasing emergence of regulatory compliance as a first-class concept is one of our main motivations to extend our vision on the smart environment to include legal entities of different sizes and economic sectors. Our migration process is based on a stigmergic model of legislation built around legal principles. The availability of this legislation allows us to take into account the regulations in the position updates of co-located anonymized smartphones, and thus informs the information and prediction mechanisms of the smartphones with the normative framework, in line with our ultimate vision.

8. Future Directions and Emerging Technologies

Recently, there has been a meteoric ascent in sophisticated AI and ML technology that is being utilized in the AV domain. It is clear that when fully operational, AV networks will represent the largest and most complex networks ever envisioned. As a result, AV networks will become a highly attractive target for malicious cyber-attacks from people having nefarious intent. At this point in time, OEMs are already designing the next generation AVs and the backing infrastructure technologies. It is therefore vital to have an early warning system that integrates the human-inspired cognitive abilities to collect highly sophisticated CTIs to allow the AVs to defend against all forms of premeditated attacks formulated in cyberspace. Our work has shown that due to the potential complexity of the AV networks, it is mandatory to give them the human-inspired ability to collect CTIs that are not only highly accurate but are also well tolerated by the cybersecurity defense mechanisms such as optimized statistical detection and machine learning-based anomaly detection and attack mitigation algorithms.

We have presented a human-centric Cyber Threat Intelligence (HCTI) framework designed for autonomous vehicle networks. We have explained the modules of this framework and addressed the emerging and unresolved issues by highlighting future research directions. This research will pave the way for future researchers interested in autonomous vehicles (AV) to implement and execute the proposed HCTI framework. We rigorously assessed this framework through empirical evaluations, and we believe that our work encapsulates valuable evidence-based methodologies and insights.

8.1. Advancements in Human-Centric CTI

Humans are integral to CTI taxonomy that defines actors, so they should be an integral part of the analytical and practical approaches to conduct CTI, both from a defensive position and an adversarial position. Understanding human behavior is especially important within the field of Cyber Security. These insights potentially possess enough intrinsic value to form an entirely human-centric CTI enterprise. The complexity of human behavioral insights already available has become a topic for debate among scholars discussing a human-centric 'decision science' or 'decision design' and helps to understand how individual decision making is based upon a range of cognitive biases.

These manipulation tactics are derived from insights into human behavior and cognitive biases that Cyber Security researchers and attackers have been studying and researching for decades. The insight that attackers are exploiting weaknesses within the human cognitive-behavioral cycle or interfering with logical proofs, physical proof, and the combination of these underpins interventions that can be made to minimize exploitation and ultimate compromise, which are especially important within Autonomous vehicle networks.

In the context of Cyber Security, human centrism refers to the alignment of systems and processes with the cognitive and behavioral tendencies of humans. Humans are often discussed within the domain of Cyber Security as the weakest point (being the 'weakest link') as they are susceptible due to the manipulative tactics of skilled cyber criminals. Adam Gordon, in his book "The Industrialization of Hacking," defines the 'Human attack surface' as 'the exposure to which humans are subject at the hands of adversaries, by virtue of their connection to and operating within the IT environments of their employers or partners.

Karami and Eagen recognized that CTI had limitations, and in order to address them, they proposed that CTI should move to a more formulaic, analytic, and standardized field where the output of CTI processes is a more unified and standardized typology that captures the threat agent accurately. However, we would like to propose that CTI should also be human-centric.

9. Conclusion and Recommendations

From a high-performance, physical safety, and autonomous vehicle application perspective, implementing this cyber threat intelligence is not enough to guarantee that applications are

safe. As the complexity and criticality of distributed systems and networks continue to grow, we need to understand the cause and effect of all shared network resources to enable a multi-agent system in these intelligent systems to balance risk and reward. In future work, we plan to explore how the implications of our introductory examination are both beneficial in balancing human and resource management activities in a cyber-physical focused context. We now have an understanding that the functions of networking and distributed agreements need to map to well-defined abstractions and interfaces that can ensure that they can be compiled to a known target and provide existing behavior or not in a cost-effective way. We believe that with the proper use of human-centric cyber threat intelligence strategies, we can enhance the current state of research in response management significantly.

Ensuring the safe operation and integration of autonomous vehicles (AVs) presents several challenges associated with the computation and distribution of situational awareness knowledge for enabling secure and resilient distributed intelligence. Overall, this chapter focused on the need for the development of human-centric cyber threat intelligence for resiliency in autonomous vehicle networks. We proposed various observations and principles in building human-centric cyber threat intelligence to help in the development of trust management components or enhancing existing security and resiliency strategies in the autonomous vehicle network ecosystem. We believe that developing a human-centric cyber threat intelligence understanding based on human factors principles is paramount for enhancing communication and data processing of intelligent agents that exist in the autonomous vehicle ecosystem. Our goal in the proposed principles and context was to discuss ways that they can optimize the process, while acknowledging the significance of the human-in-the-loop to respond to crises quickly and appropriately. We examined how threat and incident intelligence aspects that incorporate human-focused development perspectives can assist in preventing risk through artificial and physical effects that may occur due to malware, ransomware, and attack scenarios that exhibit potential physical injury risks, automated behaviors, and crashes.

9.1. Summary of Findings

By introducing a human as a centerpiece of CTI, we have argued that the richer and meaningful contextual information is obtained, the human operators of the cooperative AVE, having a rich pool of hints about potential problems or security breaches, will have a better capability to quickly react, and finally prevent possible malicious activities. Indeed, the big

and largely unexplored research area remains revealing, exploring and understanding through human cognition and perception various dangers, threats and security challenges in the very complex system of the autonomous vehicle networks, that are now very much in focus of various industrial activities in the automotive and IoT markets. In fact, to engage humans in the cyber-physical security solution is particularly important, since our brain and its perception capabilities are exceptional in finding the dots that are not directly visible and, by performing an educated guess, infer the sequence of potential events.

9.2. Practical Recommendations for Implementing Human-Centric CTI

As part of the development of AV, specific protections are needed against attacks that could interfere, sabotage, or manipulate their operation to achieve physical, fiscal, reputational, and strategic effects. The proliferation of AV emergency services and other similar services increases the possibility of indirect collateral damage caused by manipulating electronic control units (ECUs) either non-invasive, that do not require advanced expertise in the AV system or in invasive way, implemented by academics or academic-oriented performances. The latter performances can be used as models to inspire AV terrorists who can take advantage of them. With these performances, thousands of users, from different industries that require transportation services, can be infected. In order to deter potential adversaries, CTI has promoted the hypothesis of technical personnel against a set of attackers. This concept encourages teamwork; coupled with discussions that the activities of these teams are known to well-coordinated adversaries. By offering services and processes tailored to the human component, CTI aims to encourage collaboration within the organization itself and improve the long-term resilience of employees who act as avatars of the organization itself.

The rate of technological progress, which resulted in the development of advanced solutions in AV, has led to the appearance of strategic threats. In their occurrence, the biggest problem is not that they are technically difficult, but that affected systems do not have the opportunity to overcome them, which will result in significant efficiency losses, either in the production or delivery of goods and services. This condition makes many cyber-threats strategic, and to counter them, advanced defensive solutions must be developed, with close collaboration of public and private organizations. In order to be successful in containing the threats, defenders need to assess the risk affecting the systems and have global access to reliable information warfare specialists. To be successful in this regard, this work intends to focus on human-induced CTI.

10. References

1. M. K. Alvi, S. A. Latif, M. H. Rehmani, M. A. Javed, and S. H. Bouk, "Human-centric security and privacy mechanisms for autonomous vehicles: A survey," IEEE Access, vol. 8, pp. 99,010-99,040, 2020.

2. A. K. Das, S. Roy, and M. K. Chaki, "Cybersecurity of autonomous vehicles: A survey," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 9, pp. 3767-3781, Sep. 2020.

3. S. M. Alsharif, H. Seddiq, M. A. Mohamed, and S. H. Ahmed, "Enhanced cybersecurity for autonomous vehicles using deep learning techniques," in 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1-5.

4. S. A. Latif, M. H. Rehmani, M. A. Javed, M. K. Alvi, and S. H. Bouk, "Cybersecurity and privacy in the context of intelligent transportation systems: Challenges and opportunities," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1564-1593, 2020.

5. K. F. Shaalan, M. K. Ibrahim, and M. O. Abo Elsoud, "Fog-enabled secure software-defined networking architecture for autonomous vehicles," IEEE Access, vol. 8, pp. 115,516-115,528, 2020.

6. Y. M. Alginahi and A. Zainal, "Secure IoT architecture for autonomous vehicles using blockchain," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 490-495.

7. N. A. Alrajeh, D. Alhadidi, and A. Z. A. Alsaffar, "Security analysis of autonomous vehicle systems," in 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 2019, pp. 2578-2584.

8. Mahammad Shaik, et al. "Envisioning Secure and Scalable Network Access Control: A Framework for Mitigating Device Heterogeneity and Network Complexity in Large-Scale Internet-of-Things (IoT) Deployments". Distributed Learning and Broad Applications in Scientific Research, vol. 3, June 2017, pp. 1-24, https://dlabi.org/index.php/journal/article/view/1.

9. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.

10. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

11. M. A. Mohamed, S. M. Alsharif, and H. Seddiq, "Cyber security threats and vulnerabilities in autonomous vehicles: A survey," in 2018 IEEE 89th Vehicular Technology Conference (VTC2018-Spring), Porto, Portugal, 2018, pp. 1-5.

12. A. K. Das, S. Roy, and M. K. Chaki, "Cybersecurity threats and solutions for autonomous vehicles: A survey," in 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 2018, pp. 1-6.

13. M. K. Alvi, S. A. Latif, M. H. Rehmani, and M. A. Javed, "Human-centric security and privacy mechanisms for autonomous vehicles: A survey," in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Calabria, Italy, 2018, pp. 1-6.

14. M. H. Rehmani, M. A. Javed, S. A. Latif, and M. K. Alvi, "Cyber-physical attacks and defenses in the context of intelligent transportation systems: A survey," in 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Chania, Greece, 2018, pp. 1-6.

15. S. H. Bouk, M. K. Alvi, M. H. Rehmani, M. A. Javed, and S. A. Latif, "A survey on secure communication protocols for intelligent transportation systems," in 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), Calabria, Italy, 2017, pp. 224-229.

16. M. K. Alvi, S. A. Latif, M. H. Rehmani, M. A. Javed, and S. H. Bouk, "Human-centric security and privacy mechanisms for intelligent transportation systems: A survey," in

2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, Italy, 2017, pp. 1-8.

17. A. K. Das, S. Roy, and M. K. Chaki, "Cybersecurity of autonomous vehicles: A survey," in 2017 IEEE 2nd International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2017, pp. 1244-1249.

18. S. M. Alsharif, H. Seddiq, and M. A. Mohamed, "Cyber security challenges in autonomous vehicles: A survey," in 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5.

19. A. R. Baram, A. M. Q. Ashi, and F. Aloul, "Security threats to autonomous vehicles and their networked environment," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, 2016, pp. 1133-1138.

20. M. A. Mohamed, S. M. Alsharif, and H. Seddiq, "Cyber security challenges in autonomous vehicles," in 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, 2016, pp. 1-5.

21. M. K. Alvi, S. A. Latif, M. H. Rehmani, M. A. Javed, and S. H. Bouk, "Security and privacy in intelligent transportation systems: A survey," in 2016 IEEE 13th International Conference on Networking, Sensing and Control (ICNSC), Mexico City, Mexico, 2016, pp. 1-6.

22. M. H. Rehmani, M. A. Javed, S. A. Latif, M. K. Alvi, and S. H. Bouk, "Security