Bricolage ; Jurnal Magister Ilmu Komunikasi
Vol.11 (No. 1) : 59 - 74. Th. 2025
p-ISSN: 2502-0935
e-ISSN: 2615-6425

The art of deception: Mediated communication strategies in customs and excise fraud

Septian Dawang Kristanto [1*], Andre Noevi Rahmanto [1], Ignatius Agung Satyawan [1]

[1)] Master of Communication Science, Universitas Sebelas Maret, Surakarta, Jawa Tengah

Received December 23, 2024/Accepted March 06, 2025

Abstract

Current technological developments play a role in the birth of new crimes in the world, call it cybercrime. This study discusses cybercrime: fraud on behalf of Customs within the scope of persuasion communication and mediated communication from perpetrators to their victims and seen through the theory of Computer Mediated Communication (CMC) and Elaboration Likelihood Model, and also saw the campaign "beware of fraud on behalf of Customs" carried out by the Directorate General of Customs and Excise (DGCE). This research uses a qualitative approach by studying documentation related to fraud on behalf of Customs and interviewing several primary sources involved in handling the case. In addition to looking at the communication strategies implemented by the DGCE, this study will also show the development of communication patterns in the process of deception shown through the phases of impersonal, interpersonal, and hyperpersonal communication. The results of the analysis also showed that persuasion efforts emerged by fraudsters by directing their victims through peripheral routes, resulting in changes in attitude (deceived) and finally give some money to the perpetrator. Furthermore, if the peripheral route is not enough to deceive the victim, the fraudster switches to using the central route to persuade the victim through aspects of motivation, ability, and strong argumentation. This research aims to prevent people from falling victim to fraud. Addressing this issue will require cooperation from all parties, including the government, law enforcement, and the public.

Keywords: Communication Strategy; Computer Mediated Communication (CMC); Cybercrime; Fraud; Persuasion

Introduction

The rapid advancement of information and communication technology has significantly transformed the way people interact and exchange information. While these developments offer many benefits, they also present new challenges, particularly in the form of cybercrime. One prevalent issue is online fraud, which has evolved alongside digital communication platforms, making it increasingly difficult to detect and prevent. In Indonesia, fraud committed in the name of the Directorate General of Customs and Excise (DGCE) has become a widespread problem, with a growing number of victims falling prey to deceptive tactics. Despite efforts to raise awareness through public campaigns, the persistence and adaptation of fraud schemes indicate a need for a deeper understanding of the communication patterns used by perpetrators.

Existing studies on cybercrime primarily focus on legal, economic, and technological perspectives, with limited research on the role of communication strategies in fraud. This study aims to fill that gap by exploring the mediated communication techniques employed by fraudsters and analyzing the persuasion strategies they use to manipulate victims. Using the theoretical framework of Computer-Mediated Communication (CMC) and the Elaboration Likelihood Model (ELM), this research examines how fraudulent messages are structured, how victims process these messages, and what factors contribute to their susceptibility. Additionally, it evaluates the effectiveness of DGCE's public awareness campaign in mitigating fraud cases. By adopting a qualitative approach, this study seeks to provide a comprehensive understanding of fraud in the digital age, contributing to more effective prevention strategies and public education efforts.

One of the dangers referred to is the emergence of crime in cyberspace or cyber which has various modes. Most of the cybercrime we see today simply represents the migration of real-world crime to cyberspace. Cyberspace is becoming a tool that criminals use to commit old crimes in new ways (Brenner, 2010). Cyberspace is considered a safe environment for criminals to carry out

*Corresponding Author:
E-mail: awang@student.uns.ac.id

crimes by taking advantage of network security loopholes due to inefficient law enforcement (Shahbazi, 2019). The first recorded computer-mediated crime through banking was recorded in 1958, and the settlement of the case took no less than eight years, only to be completed in 1966 (Li, 2017).

The Directorate of Cyber Crime (Dittipidsiber) of the National Police Criminal Investigation Branch recorded 2,259 reports of cybercrime cases from January to September 2020. Reports related to the spread of provocative content and fraud online are the most reported. The National Police admits that handling cybercrime cases is not an easy task and requires a different approach compared to other criminal cases. Therefore, the National Police continues to strive to develop a structure with the aim of forming a Directorate of Cyber Crime in every regional police in Indonesia (Polri, 2022).

Director of Cyber Security and Cryptography for Finance, Trade, and Tourism of the State Cyber and Cryptography Agency (BSSN), Edit Prima, said that the trend of internet traffic anomalies in Indonesia showed fantastic numbers, especially in 2021 as many as 1.6 billion incidents. However, it dropped to 976.4 million incidents in 2022. Then it shrank again to 151.4 million incidents throughout 2023. The financial sector ranks third after government administration and energy, as the sector that suffers the most from internet anomalies (Okezone, 2023). BSSN invites all elements of society to always collaborate and synergize in maintaining the integrity of the national cyberspace from various cyber threats, including: ransomware, data breach, advance persistent threat, phishing, cryptojacking, distributed denial of service attack, remote desktop protocol attack, social engineering, web defacement, artificial intelligence and internet of things cybercrime (BSSN, 2023).

"Cybercrime in Indonesia is the second highest in the world after Japan. The total number of cyber attacks is 90 million," said Deputy Chief of the Indonesian National Police, Commissioner General Syafruddin in 2018 (Kominfo, 2018). (Communication and Informatics, 2018) Cybercrime has threatened Indonesian society and as mentioned above, the government and the financial sector are the top targets of crime through cyberspace. Such as fraud on behalf of Customs which is very troubling to the public with so many cases that have occurred through various types of modes. Fraud cases on behalf of Customs have continued to increase in the last five years. Based on reports related to fraud recorded by Customs, the trend of fraud complaints on behalf of Customs through *contact centers* once decreased in 2021 (after Customs carried out the campaign "Beware of Fraud on Behalf of Customs"), but it rose again and reached the highest number in 2022, reaching 7501 complaints in one year.

> "The trend of fraud complaints on behalf of Customs in the period from 2018 to 2022 had decreased in 2021 with the number of complaints reaching 2491, but increased significantly in 2022 which reached 7501 complaints," said Encep Dudi Ginanjar, Head of the Subdirectorate of Public Relations and Customs Counseling (Beacukai.go.id, 2023).

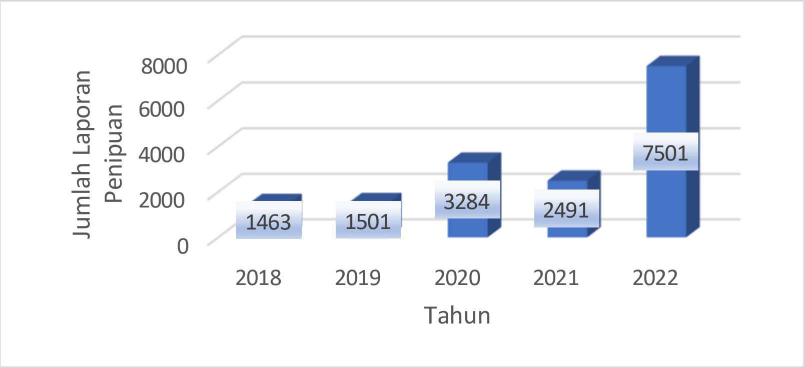


Figure 1. Fraud Report Statistics at the Customs Contact Center
Source: Customs, 2023

Prior to this study, the author first conducted a study using the Systematic Literature Review (SLR) method to see the development of studies and what research has been carried out by communication researchers in the world to examine the rampant phenomenon of cybercrime and fraud which is increasingly troubling. Through SLR research with the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) protocol, researchers found 140 Scopus studies in search using scopus.com. After that, with the help of other applications such as Mendeley, VOSViewer, and Microsoft Excel, the researchers managed to filter into 15 selected empirical studies which were then analyzed in a descriptive way.

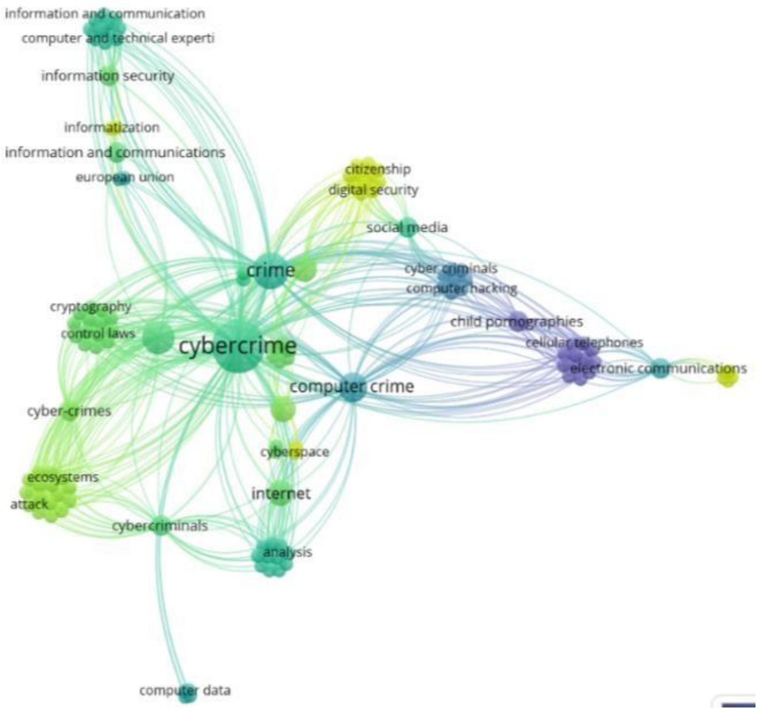


Figure 2 Network Visualization – Times
Source: Researcher, 2025

Figure two shows a network of empirical studies examining fraud and cybercrime from 2012 (purple) to 2023 (light green). The author took a fairly long time span due to the lack of journals related to fraud and cybercrime. Research in 2012 still focused on cybercrime through mobile phones and child pornography (Mthembu, 2012), progressed to 2015 and 2016 to computer hacking crimes. Developed in 2016 and 2018 began massively to cybercrime through the internet and social media (Christou, 2018; Kosseff, 2016; Nunes, 2018), peaked when 2019 to 2022 the world began to be hit by covid-19 making people stay at home and only look at gadgets all day and make cybercrime through the internet and social media increasingly rampant and unsettling (Al Ali et al., 2021; Carrillo-Mondéjar et al., 2022; Dizon & Upson, 2021; Dzhanadilov & Azhibayev, 2019; Raets & Janssens, 2021; Ruvin et al., 2020; Sin & Son, 2019). Now in 2023 2024, the world is busy talking about how the world will overcome this cybercrime by improving the internet ecosystem, cybersecurity protocols, to law enforcement and the formulation of new legal rules to eradicate cybercrime through cyberspace because it is handled very differently from crime in the real world (Althibyani & Al-Zahrani, 2023; Holovkin et al., 2023; Okhrimenko et al., 2023; Punda et al., 2023).

Figure three shows that there is still very little research on cybercrime in the government realm, which is shown by only one research relationship, between cybercrime and the government realm (cybercrime-governance).

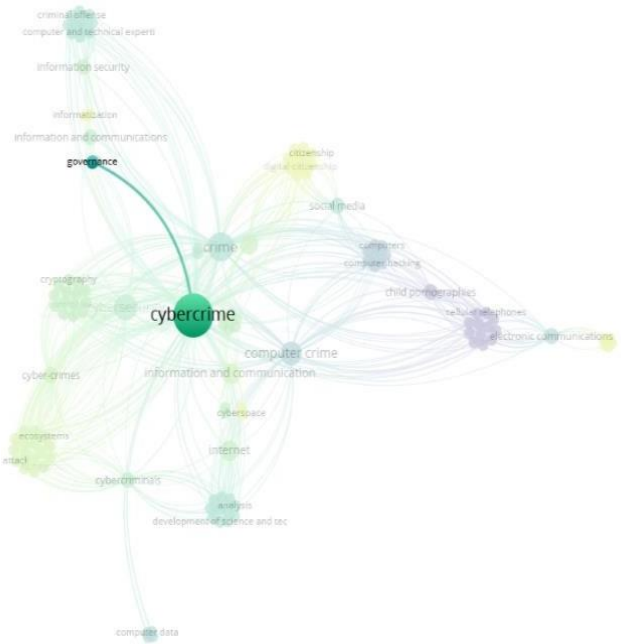


Figure 3 Network Visualization - Keywords
Source: Researcher, 2025

The findings show that cybercrime is indeed very troubling and threatens everyone through a variety of harmful and harmful ways. Through this SLR, the author found that communication research on cybercrime fraud is still limited and it is important to be carried out so that awareness and vigilance arise from the public so that they are not easily deceived. Much research has been done only on information technology, law, and economics. Many studies have been found to be qualitative, perhaps because it is difficult to get a representative sample of victims or perpetrators who want to be researched and representative.

After knowing that there are no communication researchers who have researched related to the communication patterns that occur in the fraud process, the author becomes interested and wants to find, as well as research, how mediated communication patterns occur in the process of cybercrime (fraud on behalf of Customs) through the theory of Computer Mediated Communication (CMC) by Joseph Walther. In addition, the researcher also wants to see the persuasive communication carried out by fraudsters on behalf of Customs to their victims until they are deceived through the lens of the Elaboration Likelihood Model (ELM) theory. The author is also interested in seeing the campaign "Beware of Fraud on behalf of Customs" which was successfully carried out by the Customs public relations team because it had a direct impact on reducing the number of fraud reports as soon as the campaign was carried out. This research is expected to be known by many parties so that finally awareness and vigilance from the public towards fraud which is a real, dangerous, and detrimental threat.

The phenomenon of communication through the internet, currently looks more interesting for some people than communicating face-to-face. This is referred to as hyperpersonal communication by Walther in (Juditha, 2015), which in CMC theory or communication with computer/internet intermediaries is considered more socially appealing than direct communication. According to Walther, the CMC perspective consists of three parts: impersonal, interpersonal, and hyperpersonal. Impersonal relates to the difference in the degree of acceptance of the substance of the message in the interaction, depending on the number of clues of nonverbal information available through the media. Interpersonal involves social context markers as indicators of acceptable social behavior. Meanwhile, hyperpersonalization occurs when individuals feel better expressing themselves through media that mediate interactions.

Walther stated that CMC can be more personal than face-to-face communication, exceeding the level of affection and emotion. Nonetheless, this communication pattern still has elements such as the sender of the message, the receiver of the message, the characteristics of the channel, and the feedback process, similar to conventional communication. In his theory, Walther emphasized that CMCs allow for the manipulation of messages and information (self-censorship) and provide greater control over the signals sent. Individuals use this media feature to create the best impression or counter what their contacts want.

In addition to CMC, the communication theory used by researchers to see persuasive communication in fraud on behalf of Customs institutions is the Elaboration Likelihood Model (ELM). The premise of this theory is that human beings sometimes evaluate messages in a complicated way, using critical thinking, and sometimes also do so in a simpler and less critical way (Littlejohn et al., 2021). The fraud process involves a persuasive mediated communication process, a cognitive process and ultimately influencing the victim so that they are deceived

While most studies applying ELM adopt a quantitative approach to measure attitude change, this study utilizes ELM in a qualitative context to explore the communication patterns and persuasion strategies used by fraudsters in mediated communication. Unlike traditional applications of ELM that measure persuasion effectiveness numerically, this research focuses on how fraudulent messages are structured and processed by victims. By analyzing fraud cases, the study reveals how fraudsters strategically alternate between central and peripheral routes to manipulate victims based on their level of skepticism or awareness. While ELM is predominantly used in experimental and survey-based research, previous studies have also explored its application in narrative analysis and qualitative discourse studies. For example, (Widiastuti, 2017) analyzed persuasive strategies in political communication using qualitative methods, demonstrating that ELM can be adapted to non-positivistic approaches. Similarly, Littlejohn et al. (2021) suggest that ELM is applicable in analyzing communication content where persuasion plays a key role in shaping perceptions and behaviors. This study aligns with Walther's (1996) CMC theory, which explains how online interactions influence trust and deception. Fraudsters exploit CMC features to create hyperpersonal connections with victims, leading them to rely on peripheral cues (such as urgency, authority, and credibility signals). When victims begin questioning the legitimacy of the fraud, scammers shift to the central route by presenting logical arguments and additional persuasion tactics to reinforce credibility.

Petty and Cacciopo in (Widiastuti, 2017) explaining Basically, there are two routes to explain attitude changes, namely cognitively, affective, and conative. First, the central route involves deep thinking on the message and focusing on the quality of the argument. The second route is a peripheral route that relies on clues for quick decision-making.

On the central route, the audience can judge persuasive communication as beneficial or detrimental. If the message is considered useful, the audience responds positively; Conversely, if it is considered unfavorable, a negative response is given. On the other hand, the peripheral route assumes that a change in attitude does not necessarily require an in-depth evaluation of the information presented by the media. When motivation or ability to process information is low, persuasion can occur in the periphery with simple cues that affect attitudes.

The choice between these routes has implications for the formation of attitudes. People who have the motivation, opportunity, and ability to process messages will understand the information well. Meanwhile, people who are reluctant to these three factors prefer non-message factors to form attitudes or behaviors quickly. However, such attitudes are not strong and changeable when basic factors change. These factors are known as peripheral factors, including authority, commitment, contrast, liking, reciprocation, scarcity, and social proof.

The campaign "Beware of Fraud on behalf of Customs" by Customs Public Relations is outlined in a communication strategy with the same title. In order for communication from the organization to be conveyed to the audience, the content of the message must be on target. "The success or failure of effective communication activities is largely determined by communication strategies. Strategy is essentially planning and management to achieve a goal. Strategy does not function as a roadmap that only shows direction, but must show how the operational tactics are", as Effendy said in (Anggraeni et al., 2014). Meanwhile, according to (Cangara, 2014) the communication strategy itself, it is a combination of all communication elements ranging from the sender of the message (communicator), the message, the channel (media), the receiver, to the influence (effect) which is optimally designed to achieve effective communication goals. In this study, the author uses the theory of communication strategy which is determined by the systematic ability between related components and is the answer to the map in Laswell's statement, namely who is the communicator, who is the communicator and then analyzes the needs of the audience, the message conveyed, the media used, and the expected impact (Cangara, 2014).

Method

The research method used in this study is a qualitative research method with a case study type. This research employs a qualitative approach using the instrumental case study method. A qualitative approach is used to explore and understand social phenomena, particularly how fraudsters use persuasive communication in computer-mediated interactions. This method allows the researcher to construct a detailed narrative, analyze textual and verbal communication, and gain insights into the experiences of those affected (Creswell, 2012).

The instrumental case study method is chosen because this study examines fraud on behalf of Customs not as an isolated case, but as a representation of a larger phenomenon of cyber fraud. According to Stake (1995), instrumental case studies help researchers understand broader issues by examining a specific instance in depth. By analyzing documented fraud cases and conducting interviews with experts handling such cases, this study aims to uncover persuasive strategies and mediated communication patterns that fraudsters use to deceive victims. This approach is useful for identifying trends, common techniques, and the implications of mediated fraud communication, which can contribute to developing prevention strategies and improving public awareness campaigns (Hidayat, 2017).

The characteristics of a case study involve the identification of a "case," which is a "system bound" by time and place, as well as the use of a variety of information sources to provide a detailed and in-depth picture of an event's response (Creswell, 2012). This case study method will explain the process of fraud on behalf of Customs in a detailed and in-depth way to gain a clear understanding of this phenomenon. Data collection was carried out through documentation studies from various reliable sources and in-depth interviews. Data in the form of fraud reports on behalf of Customs obtained through documentation studies from reliable sources, such as the Directorate General of Customs and Excise (DGCE) website. The documentation of the collected report is an example of a fraudulent mode on behalf of Customs with several things that must be kept secret, considering that the correspondence between the fraudster and the target is classified as confidential information in the context of law enforcement.

The information was extracted through a series of interviews with a number of informants who met the criteria, first, having an adequate understanding of the fraud process on behalf of Customs and second, having a profession specifically related to the handling of this case. The selection of informants was carried out using the purposive sampling technique. The informants consisted of two people who worked at DGCE. The first is a Head of the Communication Strategy Section of DGCE, the second informant is a DGCE Public Relations personnel who handles and participates in developing a communication strategy "Beware of Fraud on behalf of Customs".

The data analysis in this study is inductive, which means it is carried out based on the data collected. This study uses the Miles and Huberman data analysis model, which involves collecting data repeatedly until it gets data that is considered credible. The steps include data reduction to summarize, select the main points, and look for themes and patterns, presentation of data to assemble information into something easy to understand, and finally draw conclusions using the developed mindset. This study also uses descriptive analysis to describe and interpret the results of the research on communication patterns and persuasion in fraudulent schemes on behalf of Customs.

Results and Discussion

The Directorate General of Customs and Excise (Customs) is one of the institutions whose name is often used to commit *online* fraud. This can be seen from the Customs contact center service data during 2022 which shows that there are 7,501 complaints from the public who have become or are almost victims of online fraud with an estimated loss of Rp 9 billion.

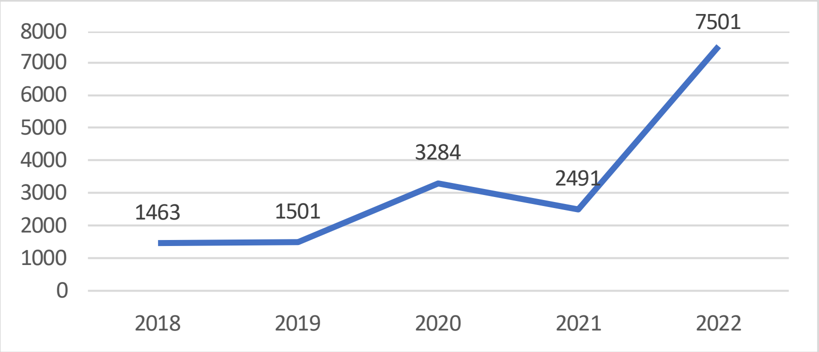


Figure 4 Trend of Fraudulent Complaints in the Name of Customs
Source: Customs, 2023

In general, fraud on behalf of Customs has a mode of perpetrators who pretend to be Customs employees or officials who detain consignments and ask for a sum of money from the victim. Some common modes of fraud on behalf of Customs include:

a. Online Shop

A fraud mode that uses the mode of buying online goods from abroad or within the country which is then conditioned as if the goods are detained by Customs and the victim is required to pay a certain amount of money.

b. Fake Auction

This mode of fraud ensnares victims with fake auctions of goods confiscated by Customs that are sold at low prices. The victim was asked to make a payment, even though the item being auctioned was fictitious/non-existent.

c. Romance Scams

This mode is carried out with an intense and romantic approach, for example claiming to be a wealthy businessman from the United Arab Emirates or an Army General from the United States who promised to come to Indonesia to marry the victim, also promising to send gifts/valuables to the victim who was then detained for the goods and needed to be paid to the perpetrator who claimed to be Customs.

d. Diplomatic Goods

This mode is carried out by getting acquainted with the victim who then pretends to send carrying valuables through diplomatic channels. Then, the victim was asked to transfer a sum of money on the grounds that it was detained at Customs.

In addition to the four general modes above, new modes also continue to emerge following changes in the situation/policy. One of the last examples is when Customs implements *an electronic customs declaration* (e-CD) and then a new fraud mode is born with the emergence of fake websites for filling out e-CDs that turn out to steal the personal data of the victims and finally ask for payment of a sum of money.

There are three factors that make computer communication more attractive to communication partners, namely: (1) social media, e-mail and other forms of communication allow for highly selective self-presentation, with fewer unwanted appearances or behaviors compared to direct communication. It is easier for people not to put on a look and bother hiding their bad traits when communicating over the internet; (2) People who engage in computer-mediated communication sometimes tend to make excessive attribution in forming a stereotypical impression of their communication partner. This kind of conclusion tends to ignore negative information such as typographical errors, typos, and other types of errors; and (3) an intensification bond may arise, where positive messages from a communication partner will trigger other positive messages (Juditha, 2015).

Computer-Mediated Communication (CMC) in Fraud

During an interview with an informant from Customs, TT said that fraud cases by profiteering the name of Customs institutions have taken many victims, ranging from women to men, teenagers to the elderly, from low education to highly educated. He also explained that the *online shop* and romance fraud modes are the second largest modes reported so far. The impersonal phase in fraud on behalf of Customs is mostly a request for the transfer of funds for consignments held at Customs (online shop mode). In romance mode, we can see it too, when a scammer suddenly invites acquaintances through direct messages on social media such as Instagram or Facebook through sweet and flattering sentences, so that the unknown person is relieved and wants to make friends. Impersonal is a phase of interpersonal relationships where each other does not know each other, communication interaction is two-way (verbal and nonverbal), exchanging messages and feelings. After the relationship is formed, the communication pattern is directed towards deeper interaction, the impostor who as a communicator begins to unleash his deception using romantic, more open, and more intimate words. The relationship between the scammer and the potential victim can be formed so quickly that it becomes familiar, this is due to the fact that communication through CMC feels more impersonal compared to face-to-face communication. (M. Walther et al., 2023) explained that this method feels more personal and even exceeds the level of affection and emotion compared to face-to-face communication. Therefore, in general, people tend to prefer internet- or computer-mediated communication over face-to-face.

When a person communicates with strangers online, such as through direct messages or social media chat rooms, the individual can form a perception of the person he or she is talking to based on grammar, writing style, content of the conversation, the appearance of the profile picture and other factors (even though everything is not genuine and many bad traits are not shown). If the interlocutor is considered handsome/beautiful, smart, fun, and easy to talk to, then effective communication can be formed. Otherwise, the interaction may not go smoothly. Furthermore, involvement in highly intimate interactions can occur, even without the communicator's knowledge that they may be falling into the trap of deception.

Not only through the impersonal phase, fraud on behalf of Customs also develops through the interpersonal phase. Taylor in (Juditha, 2015) said effective interpersonal communication consists of many elements, but interpersonal relationships are the most important. CMC is one of the sources in improving the quality of communication. Moreover, interpersonal communication is growing with the existence of the internet with various facilities that allow users to have direct contact. In the interpersonal phase, the exchange of information between communicators and communicators increases as they spend more time communicating. The perpetrator as a communicator focuses on trying to find information about the victim in order to get complete information (Andriyanto, 2022). It was mentioned in an interview with TT that victims increasingly fell into the trap of fraud day by day, always being asked for news, stories through video calls, especially after being promised luxury gifts such as electronics, jewelry, cash, houses, and even promised to marry. Until this interpersonal phase, usually the victim has begun to be deceived but still believes that the person he has just met and has become his lover can still be trusted. As stated by (Walther, 1996), CMCs have the ability to manipulate messages and information (self-censorship), providing greater control over the signals sent. Thus, it can be seen that the scammers are able to control the situation through the manipulation of their messages, so that the victim is trapped. Over time, the recipient of the message tends to be affected and often ignores the negative information that appears.

The last phase is hyperpersonal where hyperpersonal communication in fraud on behalf of Customs is based on four main factors, namely the source of the message, the recipient of the message, the channel, and the feedback. The source of the message shows that the scammers have complete control over their self-presentation. In communication situations with their victims, scammers manage to create the best image of themselves, including personality, achievements, and even appearance, this can happen in mediated communication without meeting face-to-face. In this scam, the recipient of the message who feels lonely and is looking for a mate is often captivated by the presentation (handsome/beautiful, caring, successful, and rich) and without hesitation gives positive feedback. This builds intense communication, and the victim quickly falls into the trap.

The hyperpersonal phase of fraud in the name of Customs occurs when even though the communicator and communicator are separated and only carry out computer-mediated communication, the perpetrator can build a perfect self-presentation and change his communication style. Scammers cleverly use various messaging channels, such as social media or messaging apps to make it easier to achieve their goals. Initially, they may only communicate via email or chat rooms, but as familiarity with potential victims increases, they exchange phone numbers to increase closeness. Through positive feedback from victims to their messages, the scammers manage to establish good communication and lead victims on a positive path, achieving their fraudulent goals.

Persuasive Communication in Fraud: ELM Application

Not only impersonal, interpersonal, and hyperpersonal, the fraud process is increasingly undergoing a transformation into a more interactive and convincing pattern effectively. The modes that have been known to the public make the fraudsters increasingly look for ways and use more persuasive communication to be able to deceive their potential victims.

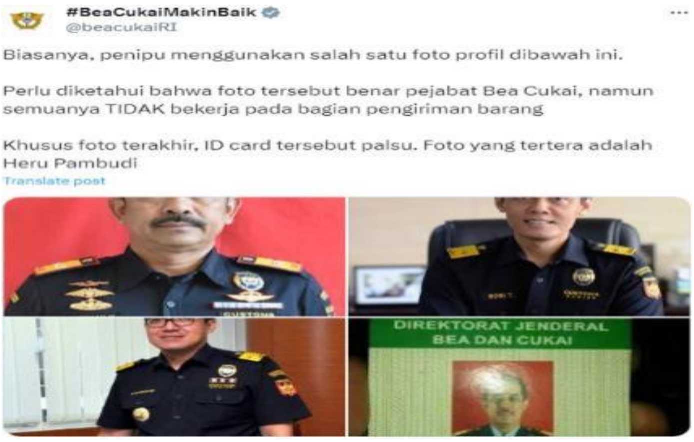
Persuasive communication in fraud on behalf of Customs can be explained through the theoretical concept of the ELM. The ELM published by Richard Petty and John Cacioppo discusses how communicators process persuasive messages. The basis of this ELM is that humans will evaluate the messages received in two ways, either by elaborating critically through the central route or by thinking more simply through the peripheral route. The selection of the route will also determine whether there is a change in attitude in the recipient of the message (Littlejohn et al., 2021).

If the victim of fraud on behalf of Customs chooses the central route, the message received will go through several stages before a change in attitude occurs. The stages include (1) motivation, which involves the personal relevance of the message and the need for cognition, which is the enjoyment of thinking about a message even if the message is not actually personally relevant; (2) ability, which includes the ability to overcome distractions and adequate understanding, with the possibility of objective elaboration and bias elaboration; and (3) the power of argumentation, where strong arguments encourage attitude change, while neutral and weak arguments do not change attitudes, can even reinforce opposing viewpoints (Littlejohn et al., 2021).

On the other hand, peripheral routes will be chosen without involving complex elaboration and without going through a number of stages. This route only requires one or a few cues to produce a change in attitude. Peripheral routes are another way for fraudsters to persuade their victims to change their attitudes. However, changes in attitude through peripheral routes tend to be temporary and can only meet temporary needs.

Persuasion in fraud in the name of Customs in addition to the mode of romance in principle seeks to encourage the victim to receive the message through peripheral routes. The choice of this route was carried out because the scammer mainly aimed to make a profit quickly, in contrast to romance mode fraud that was carried out for a long time. If the victim realizes that he has been deceived, the perpetrator immediately removes his traces and immediately continues to look for the next target of the operation. Peripheral routes can be executed by relying on one or more specific cues, for example:

a. Gesture of authority



#BeaCukaiMakinBaik
@beacukaiRI

Biasanya, penipu menggunakan salah satu foto profil dibawah ini.

Perlu diketahui bahwa foto tersebut benar pejabat Bea Cukai, namun semuanya TIDAK bekerja pada bagian pengiriman barang

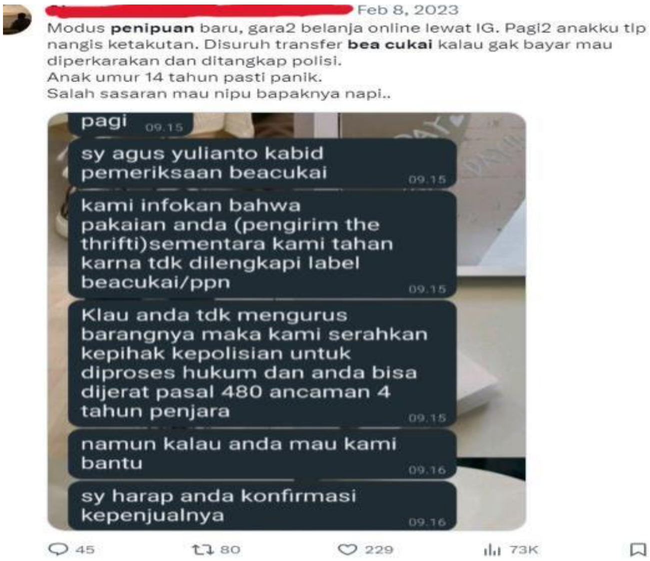
Khusus foto terakhir, ID card tersebut palsu. Foto yang tertera adalah Heru Pambudi

Translate post

Figure 5 Persuasion of Authority Signals
Source: @beacukairi, twitter.com, 2023

By using a fake identity, the fraudster creates the impression that as a Customs official, the fraudster guides the victim to immediately carry out the request (order) submitted. Because of fear and panic, victims tend to obey orders from the authorities without much consideration and without verifying the validity of their identity.

b. Scarcity tactics



[redacted] Feb 8, 2023

Modus **penipuan** baru, gara2 belanja online lewat IG. Pagi2 anakku tip nangis ketakutan. Disuruh transfer **bea cukai** kalau gak bayar mau diperkarakan dan ditangkap polisi.
Anak umur 14 tahun pasti panik.
Salah sasaran mau nipu bapaknya napi..

pagi 09.15

sy agus yulianto kabid pemeriksaan beacukai 09.15

kami infokan bahwa pakaian anda (pengirim the thrifti)sementara kami tahan karna tdk dilengkapi label beacukai/ppn 09.15

Klau anda tdk mengurus barangnya maka kami serahkan kepihak kepolisian untuk diproses hukum dan anda bisa dijerat pasal 480 ancaman 4 tahun penjara 09.15

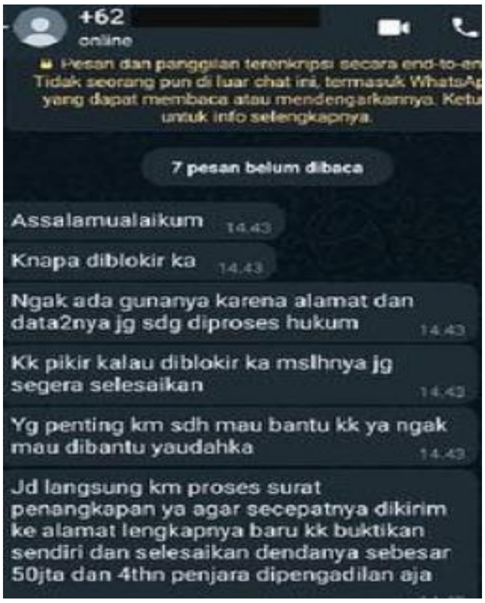
namun kalau anda mau kami bantu 09.16

sy harap anda konfirmasi kepenjualnya 09.16

Figure 6 Persuasion of Scarcity Signals
Source: X, twiter.com, 2023

This gesture is used for urgent persuasion and is almost always used in persuasive communication, making the interlocutor carry out the communicator's commands without going through the perfect thought process. By conveying the wrong message, fraudsters create the impression that it is very important and must be carried out in the shortest possible time. For example, in Figure 6, the perpetrator directs to immediately take care of his belongings by fearing that the victim will be processed by law.

c. Contrast cues



+62 [redacted]
online

Pesan dan panggilan terenkripsi secara end-to-en
Tidak seorang pun di luar chat ini, termasuk WhatsAp
yang dapat membaca atau mendengarkannya. Ketu
untuk info selengkapnya.

7 pesan belum dibaca

Assalamualaikum 14.43

Knapa diblokir ka 14.43

Ngak ada gunanya karena alamat dan data2nya jg sdg diproses hukum 14.43

Kk pikir kalau diblokir ka mslhnya jg segera selesaikan 14.43

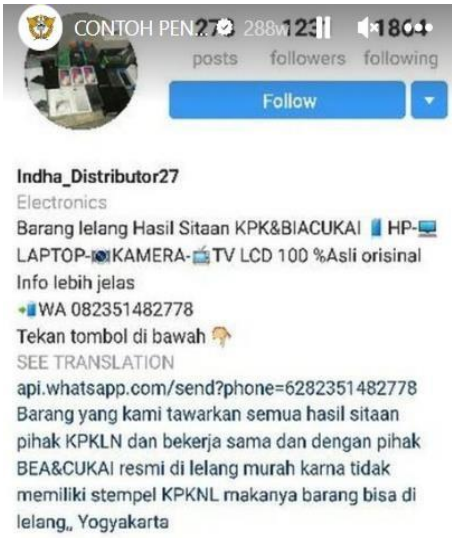
Yg penting km sdh mau bantu kk ya ngak mau dibantu yaudahka 14.43

Jd langsung km proses surat penangkapan ya agar secepatnya dikirim ke alamat lengkapnya baru kk buktikan sendiri dan selesaikan dendanya sebesar 50jta dan 4thn penjara dipengadilan aja

Figure 7 Persuasion of Contrasting Signals
Source: Y, twiter.com, 2023

The gesture is used in a way as if this perpetrator wants to offer services to help the victim, but on the other hand threatens to make payment immediately if he does not want to be fined and sentenced to prison, it looks like he wants to help, even though he is deceiving as seen in Figure 7; or

d. Credibility Manipulation



Indha_Distributor27
Electronics
Barang lelang Hasil Sitaan KPK&BIACUKAI 📱 HP-💻
LAPTOP-📷KAMERA-📺TV LCD 100 %Asli orisinal
Info lebih jelas
➡📱WA 082351482778
Tekan tombol di bawah 👇
SEE TRANSLATION
api.whatsapp.com/send?phone=6282351482778
Barang yang kami tawarkan semua hasil sitaan
pihak KPKLN dan bekerja sama dan dengan pihak
BEA&CUKAI resmi di lelang murah karna tidak
memiliki stempel KPKNL makanya barang bisa di
lelang,, Yogyakarta

Figure 8 Persuasion of Credibility Signals
Source: beacukairi, instagram.com, 2023

Scammers boldly convey a credible message even though it is a lie. As can be seen in Figure 8, the fraudster said that he sold goods confiscated by Customs and the KPK where we know that they do not exist, cannot be sold without going through an official auction channel. However, it turns out that the perpetrator's goal is to target potential victims who are greedy and want the price to be too cheap, so rationality is sidelined, and falls into the trap of fraudsters.

The use of persuasion through peripheral routes by utilizing a certain number of cues as mentioned above can speed up the communication process and change the attitude of the message recipient. In some cases of fraud on behalf of Customs, the transfer of funds to the account provided by the bad actor is carried out very quickly as a result of this strategy. In its implementation, fraudsters on behalf of Customs not only direct persuasion efforts to peripheral routes, but also use central routes because there are different responses from victims to messages received by fraudsters. According to TT from Customs, the latest mode of fraud practices on behalf of Customs has begun to use technology, such as *phishing* application *tracking* fake made by fraudsters and so on, to be able to trap faster without going through many conversations, because through the campaign "Beware of Fraud on the Behalf of Customs", the public has a better understanding of the regulations and knows the modes of fraud that are commonly carried out by fraudsters. This process takes less time for the victim to understand the communication and persuasion carried out by the perpetrator and eventually falls into the trap of fraud. In this situation, the perpetrator forms appropriate motivational and understanding steps, develops sufficient skills and understanding, and devizes a strong argument. If it turns out that the central route does not result in a change in attitude on the victim, the BEC perpetrator will repeat the communication process from the beginning and refocus on the peripheral route. Through the findings and discussion above, the author tries to describe a persuasive communication model in the phenomenon of fraud on behalf of Customs as shown in Figure 9. In the image below, we can see that the communication process that occurs in fraud on behalf of Customs appears after the target, the potential victim has been determined, through excavation and collection of information data through *Social Engineering* (manipulation of the victim's psychology in the mode of romance), *Pharming* (directing the victim to a fake site in the mode of *fraudulent online shops*, fraudulent auctions).

Bricolage ; Jurnal Magister Ilmu Komunikasi
Vol.11 (No. 1) : 59 - 74. Th. 2025
p-ISSN: 2502-0935
e-ISSN: 2615-6425

Persuasive communication begins with impersonal communication (initial acquaintance and communication), followed by interpersonal and hyperpersonal communication. Persuasive communication is carried out in an effort to direct the victim to the peripheral route through various cues (authority, rarity, contrast, credibility and others). Not only stopping there, fraudsters have also provided another alternative way, namely persuasive communication directed to the central route if the peripheral route built does not succeed in deceiving the victim. If persuasive communication also does not succeed, the fraudster will repeat the persuasive communication process until the victim falls into the trap of fraud and the fraudster achieves his goal.

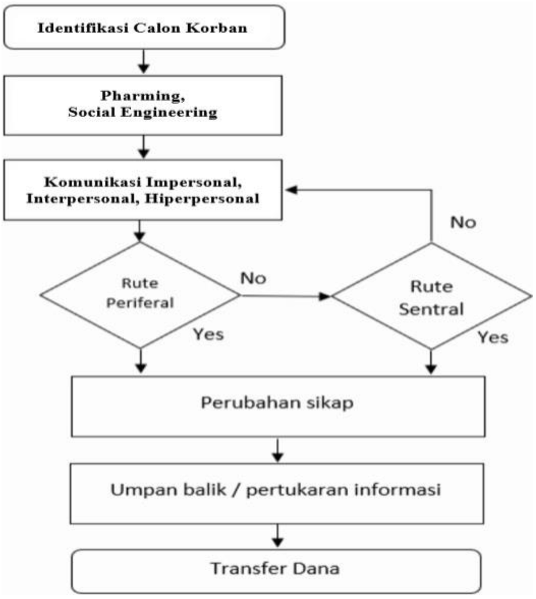


Figure 9 Fraudulent Persuasion Communication Model on behalf of Customs
Source: Processed by Researcher, 2025

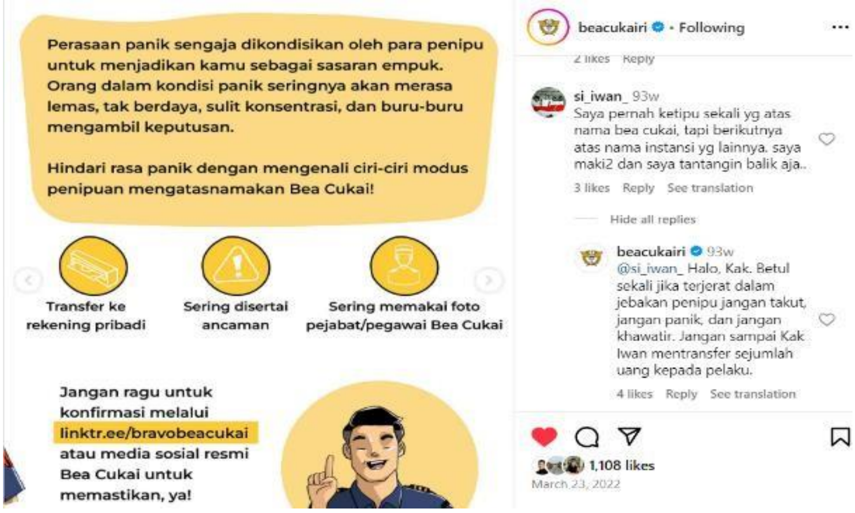
Impact of Customs' Awareness Campaign

The DGCE or commonly called Customs has implemented several communication strategies to handle the issue of fraud on behalf of its institution even though it has only been carried out in a structured manner since 2022. The purpose of the communication strategy carried out so far is to increase public awareness of fraud on behalf of Customs with key messages based on its audience, both internal and external. For internally, the key messages conveyed are the modes of fraud and appeals to convey this information to the environment around employees. For external, the messages conveyed by Customs are in the form of fraud modes and their characteristics, duties and authorities of Customs as well as Customs information contacts for confirmation.

The communication tactics that have been implemented by Customs are also diverse, both in the form of social media uploads, socialization, talk shows, news articles, and others. For social media uploads and news articles, Customs conducts published on a scheduled basis to fill the digital space with related information. This tactic is also encouraged by *paid promotions* to encourage tactical reach. For socialization, Customs carries out this tactic both directly and online. Customs also takes advantage of visits from schools to Customs offices by inserting and disseminating fraudulent alert messages on behalf of Customs. Customs is also unfortunate to cross the National and Regional Television and Radio talk shows by continuing to voice vigilance of fraud on behalf of Customs. Then, Customs also claims to continue to make collaborative efforts. Some of the communication or collaboration efforts with external parties are carried out, including:

a. Coordination with the Ministry of Communication and Information regarding websites that profit from the name of Customs;
b. Coordination with the Financial Services Authority related to the existence of accounts in the name of Customs;

c. Communication with the Indonesian National Police related to the legal handling of fraud on behalf of Customs;
d. Communication with social media (facebook) to eliminate social media accounts on behalf of Customs to commit fraud;
e. In the implementation of the communication strategy, the Customs also revealed several obstacles, as follows: Limited data, Customs collects data through complaints and independent surveys; Limited resources, related to the availability of resources and funds in carrying out communication tactics or collaborating with influencers; Limitations of collaboration, related to the differences in priorities of each party in handling this issue which hinders collaboration efforts;



Perasaan panik sengaja dikondisikan oleh para penipu untuk menjadikan kamu sebagai sasaran empuk. Orang dalam kondisi panik seringnya akan merasa lemas, tak berdaya, sulit konsentrasi, dan buru-buru mengambil keputusan.

Hindari rasa panik dengan mengenali ciri-ciri modus penipuan mengatasnamakan Bea Cukai!

Transfer ke rekening pribadi

Sering disertai ancaman

Sering memakai foto pejabat/pegawai Bea Cukai

Jangan ragu untuk konfirmasi melalui linktr.ee/bravobeacukai atau media sosial resmi Bea Cukai untuk memastikan, ya!

beacukairi • Following

2 likes Reply

si_iwan_ 93w
Saya pernah ketipu sekali yg atas nama bea cukai, tapi berikutnya atas nama instansi yg lainnya. saya maki2 dan saya tantangin balik aja..
3 likes Reply See translation

Hide all replies

beacukairi 93w
@si_iwan_ Halo, Kak. Betul sekali jika terjerat dalam jebakan penipu jangan takut, jangan panik, dan jangan khawatir. Jangan sampai Kak Iwan mentransfer sejumlah uang kepada pelaku.
4 likes Reply See translation

1,108 likes
March 23, 2022

Figure 10 Example of a Fraud Alert Campaign on the Behalf of Customs
Source: Instagram (@BEACUKAIRI, 2023)

The researcher tries to describe the communication strategy that has been carried out by DGCE in campaigning, socializing, and providing education to the public regarding fraud vigilance on behalf of Customs by using good communication theory according to Hafied Cangara (Cangara, 2014).

a. The communicator appointed in an effort to convey information to the public is the spokesperson of the DGCE institution, namely the Director of Communication and Guidance for DGCE Service Users. However, it is hoped that all DGCE employees will be able to become a mouthpiece to disseminate information related to fraud vigilance on behalf of Customs, so that *awareness* emerges from the public, knows the correct procedures, and will not be easily deceived and deceived by fraud mode.
b. The target audience of message recipients in the socialization of fraud on behalf of Customs is all levels of society who actively interact on the internet, people who actively shop online, cannot be limited in terms of demographics: in terms of age, gender, and education level, because both young or old, men or women, higher and lower education, all are still vulnerable to becoming victims of fraud according to research conducted by DGCE.
c. After determining the communicator, and the target audience of the message recipient, the creation of the message itself becomes key. The communication message conveyed by DGCE contains information and education about fraud modes on behalf of Customs, procedures for paying import duties and taxes in the context of correct imports, do not panic, and then when the public is in doubt about certain information related to Customs and Excise do not hesitate to contact the official communication channel of the Customs Contact Center 1500225.
d. The communication media used by Customs Public Relations are online media such as Instagram, Twitter, Facebook, Tiktok, official websites, then Customs' media channels, namely the Radio and Tv Customs Channels and also Customs have the opportunity to collaborate with mass media such as TV, Radio, as well as national print and online media.

e. The expected communication effect after carrying out and evaluating the socialization efforts of "Beware of Fraud on behalf of Customs" is to be able to prevent fraud from happening again and break the chain of fraud on behalf of Customs, straighten out negative assumptions in the public towards Customs and can eliminate public doubts to contact the communication channels owned by Customs when receiving suspicious information.

Conclusion

Fraud on behalf of Customs is generally carried out through online communication, especially through social media and messaging applications. Mediated communication via the internet from the scammer to the potential victim results in a communication process that is initially impersonal, then develops into interpersonal communication which is characterized by an increase in communication activities, even reaching the level of hyperpersonal communication, where the victim feels close and trusts the perpetrator even though it is only through an intermediary without face-to-face. This evolution from the impersonal to the interpersonal stage is influenced by the persuasion efforts embedded in the messages sent. In general, scammers try to influence victims through light peripheral signals, such as authority signals, rarity, contrast, and credibility signals.

Fraudsters can carry out alternative plans through a central route approach, while fraudsters still try to build communication by utilizing indicators in the central route, including motivation, ability, and argumentation. If the victim begins to perform cognitive processes and becomes suspicious, the perpetrator will try to redirect the victim back to the peripheral route by using a number of light signals that attract attention.

This fraud is a problem that does not only exist in Indonesia, because of the transnational nature of the crime. Countermeasures require a comprehensive approach that involves various views, such as legal, regulatory, economic, IT, and communication understanding. Effective cooperation between all stakeholders with uniform knowledge and views is essential so that this crime does not develop and can be stopped. As a concrete step, DGCE has carried out a campaign through the implementation of the communication strategy "Beware of Fraud on behalf of DGCE" appropriately which is preceded by communication research to determine communicators, target audiences, message making, communication channel selection, and evaluation monitoring to analyze communication effects.

References

Al Ali, N. A. R., Chebotareva, A. A., & Chebotarev, V. E. (2021). Cyber Security In Marine Transport: Opportunities And Legal Challenges. *Pomorstvo*, *35*(2), 248–255. Https://Doi.Org/10.31217/P.35.2.7

Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating The Effect Of Students' Knowledge, Beliefs, And Digital Citizenship Skills On The Prevention Of Cybercrime. *Sustainability (Switzerland)*, *15*(15). Https://Doi.Org/10.3390/Su151511512

Andriyanto, T. (2022). Fraud Mediated Communication With Business Email Compromise Mode. *Journal Of Communication Research*, *5*(2), 220–243.

Anggraeni, N., Siswoyo, M., & Nurfalah, F. (2014). Public Relations Strategy In Supporting The Marketing Of National Power Plants (Pln). *Aspikom Journal*, *2*(3), 206–220.

Beacukai.Go.Id. (2023, December 29). *This Is An Effort By Customs To Prevent Fraud On Behalf Of The Institution*. Https://Www.Beacukai.Go.Id/Berita/Ini-Upaya-Bea-Cukai-Cegah-Penipuan-Mengatasnamakan-Institusi.Html

@Beacukairi. (2023). *Social Media Of The Directorate General Of Customs And Excise*. Beacukai.Go.Id

Brenner, S. W. (2010). *Cybercrime: Criminal Threats From Cyberspace*. Praeger.

Bssn. (2023). *Annual Report*.

Cangara, H. (2014). *Communication Planning And Strategy*. King Grafindo Persada.

Carrillo-Mondéjar, J., Martinez, J. L., & Suarez-Tangil, G. (2022). On How Voip Attacks Foster The Malicious Call Ecosystem. *Computers And Security*, *119*. Https://Doi.Org/10.1016/J.Cose.2022.102758

Christou, G. (2018). The Challenges Of Cybercrime Governance In The European Union. *European Politics And Society*, *19*(3), 355–375. Https://Doi.Org/10.1080/23745118.2018.1430722

Creswell, J. (2012). *Qualitative Inquiry And Research Design: Choosing Among Five Approaches* (3rd Ed.). Sage.

Dizon, M. A. C., & Upson, P. J. (2021). Laws Of Encryption: An Emerging Legal Framework. *Computer Law And Security Review*, *43*. Https://Doi.Org/10.1016/J.Clsr.2021.105635

Dzhanadilov, O. M., & Azhibayev, M. G. (2019). Problems Of Countering Criminal Offenses In Information And Communication Networks. *Journal Of Advanced Research In Law And Economics*, *10*(1), 134–143. Https://Doi.Org/10.14505/Jarle.V10.1(39).14

Hidayat, M. (2017). Kyai Communication Model With Students In Islamic Boarding Schools. *Aspikom Journal*, *2*(6), 385. Https://Doi.Org/10.24329/Aspikom.V2i6.89

Holovkin, B., Cherniavskyi, S., & Tavolzhanskyi, O. (2023). Factors Of Cybercrime In Ukraine. *Relacoes Internacionais No Mundo Atual*, *3*(41), 464–488. Https://Doi.Org/10.21902/Revrima.V3i41.6401

Juditha, C. (2015). Communication Patterns In Cybercrime (Love Scams Case) Communication Patterns In Cybercrime (Love Scams Case) Communication Patterns In Cybercrime (Love Scams Case). *Journal Of Communication And Informatics Research And Development* , *6*(2).

Kominfo. (2018, July 18). *National Police: Indonesia Is The Second Highest Cybercrime In The World*. Https://Www.Kominfo.Go.Id/Content/Detail/13487/Polri-Indonesia-Tertinggi-Kedua-Kejahatan-Siber-Di-Dunia/0/Sorotan_Media

Kosseff, J. (2016). The Hazards Of Cyber-Vigilantism. *Computer Law And Security Review*, *32*(4), 642–649. Https://Doi.Org/10.1016/J.Clsr.2016.05.008

Li, J. X. (2017). Cyber Crime And Legal Countermeasures: A Historical Analysis. *International Journal Of Criminal Justice Sciences*, *12*(2). Https://Doi.Org/10.5281/Zenodo.1034658

Li, X. (2016). Regulation Of Cyber Space: An Analysis Of Chinese Law On Cyber Crime. *International Journal Of Cyber Criminology*, *9*(2). Https://Doi.Org/10.5281/Zenodo.56225

Littlejohn, S. W., Foss, K. A., & Oetzel, J. G. (2021). *Theories Of Human Communication* (Twelfth Edition). Waveland Press, Inc.

Mthembu, M. A. (2012). High Road In Regulating Online Child Pornography In South Africa. *Computer Law And Security Review*, *28*(4), 438–444. Https://Doi.Org/10.1016/J.Clsr.2012.05.010

Nunes, D. R. (2018). The Means Of Obtaining Evidence Provided By The Portuguese Cybercrime Law (Law No. 109/2009 Of 15 September 2009). *Comparative Law Review*, *24*, 249–286. Https://Doi.Org/10.12775/Clr.2018.010

Okezone. (2023, December 30). *Cybercrime Threatens The Financial Industry, Bssn: There Were 151.4 Million Incidents During 2023*.

Okhrimenko, I., Stepenko, V., Chernova, O., & Zatsarinnaya, E. (2023). The Impact Of Information Sphere In The Economic Security Of The Country: Case Of Russian Realities. *Journal Of Innovation And Entrepreneurship*, *12*(1). Https://Doi.Org/10.1186/S13731-023-00326-8

Police. (2022). *Cybercrime In Indonesia Has Increased Many Times*.

Punda, O., Vavrynchuk, M., Kohut, O., Kravchuk, S., & Prysiazhniuk, M. (2023). The Legal Status And Capabilities Of Cyber Police In Ukraine: The Reasons For The Existence Of Frauds With The Use Of It Technologies. *Pakistan Journal Of Criminology*, *15*(2), 165–180.

Https://Www.Scopus.Com/Inward/Record.Uri?Eid=2-S2.0-85167433844&Partnerid=40&Md5=667cb4ce9172abcbf31894ab08738682

Raets, S., & Janssens, J. (2021). Trafficking And Technology: Exploring The Role Of Digital Communication Technologies In The Belgian Human Trafficking Business. *European Journal On Criminal Policy And Research*, *27*(2), 215–238. Https://Doi.Org/10.1007/S10610-019-09429-Z

Ruvin, O., Isaieva, N., Sukhomlyn, L., Kalachenkova, K., & Bilianska, N. (2020). Cybersecurity As An Element Of Financial Security In The Conditions Of Globalization. *Journal Of Security And Sustainability Issues*, *10*(1), 175–188. Https://Doi.Org/10.9770/Jssi.2020.10.1(13)

Shahbazi, A. (2019). Technological Developments In Cyberspace And Commission Of The Crimes In International Law And Iran. In *Journal Of Legal, Ethical And Regulatory Issues* (Vol. 22, Issue 4).

Sin, J.-M., & Son, H.-R. (2019). Dealing With The Problem Of Collection And Analysis Of Electronic Evidence. *International Journal Of Electronic Security And Digital Forensics*, *11*(3), 363–377. Https://Doi.Org/10.1504/Ijesdf.2019.100497

Walther. (1996). Computer Mediated Communication: Impersonal, Interpersonal, And Hypersonal Interaction. *Communication Research*, *3*(43).

Walther, M., Jakobi, T., Watson, S. J., & Stevens, G. (2023). A Systematic Literature Review About The Consumers' Side Of Fake Review Detection – Which Cues Do Consumers Use To Determine The Veracity Of Online User Reviews? *Computers In Human Behavior Reports*, *10*, 100278. Https://Doi.Org/Https://Doi.Org/10.1016/J.Chbr.2023.100278

Widiastuti, T. (2017). Analysis Of The Elaboration Likelihood Model In The Formation Of Ridwan Kamil's Personal Branding On Twitter. *Aspikom Journal*, *3*(3), 588–603. Http://Databoks.Katadata.