Association for Information Systems

AIS Electronic Library (AISeL)

WHICEB 2019 Proceedings | Wuhan International Conference on e-Business

Summer 6-26-2019

A Review on Cognitive Neuroscience in Information Security Behavior

Zhiying Wang
College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, 212000, China, wangzy_20066@163.com

Hangyu Deng
College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, 212000, China

Nianxin Wang
College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, 212000, China

Shilun Ge
College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, 212000, China

A Review on Cognitive Neuroscience in Information Security Behavior

Zhiying Wang[1*] *Hangyu Deng*[1] *Nianxin Wang*[1] *Shilun Ge*[1]

[1]College of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang, 212000, China

Abstract: NeuroIS is a hot topic of research in recent years, and cognitive neuroscience has found a new way to explain the underlying causes of human behavior in the field of information security research. By searching the research status of cognitive neuroscience in information security behavior research, we found that the number is gradually increasing, and the most frequently used neurocognitive tools are fMRI, EEG and eye tracking. Then a brief description of the application of each tool. Through combing the existing literature, it is found that cognitive neuroscience has become an important research subdomains in the information security behavior, and the research context has been clarified, which has provided guidance for subsequent research.

Keywords：information security behavior, neuroscience, EEG, eye tracking, fMRI,

1. INTRODUCTION

The concept of NeuroIS was proposed by Dimoka, Pavlou et al. at the 2007 International Information Systems Conference, an interdisciplinary field of research between neuroscience and information systems[1]. Cognitive neuroscience theories, methods, and related neuroscience tools can guide the research of information system behavior, complement the existing information system research methods, and cognitive neural tools can also provide objective data which questionnaires, archival data and other traditional research methods difficult to obtain[2]. The research on the neural mechanism of the tools of cognitive neuroscience is the help of the research on behavior and emotion in the field of information systems and is getting more and more scholars in the information field.

With the interaction between cognitive neuroscience and information systems, information security scholars have begun to study the neural mechanism of information security behavior in recent years. The reason is that with the development of information technology and people's dependence on information technology, information system security has become a research hotspot in the field of information systems. Existing research has gradually recognized that individual users play an important role in the security of information systems because users are the weakest link in system security, user negligence or deliberate behavior can lead to security threats to information systems. However, most information security behaviors and motivations of users in existing research are based on self-reported interviews and surveys, and many factors make this kind of self-reported survey biased, which affects the correctness of scholars' research on information security behavior, such as information security. People in the background usually do not admit their unethical behavior or make a distorted record of behavior in consideration of their image or work in the organization[3]. Although cognitive neuroscience has supplemented this problem and the rapid development of information system security behavior research has been promoted, but the behavioral research of cognitive neuroscience in information security is still in the early stages of development. Therefore, summarizing the research topics, research methods and research status of cognitive neuroscience in the field of information security have great significance for clarifying the research and carrying out research on NeuroIS in the future. This paper combs the development status of the field of NeuroSec, reviews and summarizes it.

* Corresponding author. Email: wangzy_20066@163.com (Zhiying Wang)

2. LITERATURE RETRIEVAL AND ANALYSIS

We used key terms representing the field as a whole such as "information security & EEG", " security warning & NueroIS" and "phishing & eye tracking" et.al for our research; through the keyword search of Springer, EBSCOhost, AIS, ScienceDirect, EI, and other databases, a total of 18 papers using cognitive neuroscience in information security behavior research are found, and the result show research time is up to 2011-2019. They are published in top journals and international conferences in the field of information systems such as MIS Quarterly, Journal of Management Information Systems (JMIS), Information Systems Research (ISR), Journal of Association for Information Systems (JAIS), and two of JMIS and JAIS. We also found that Bonnie Brinton Anderson published four related studies, Anthony Vance published three related research papers, and Qing Hu published two related research papers. As shown in Figure 1, through the review of the literature can be found that 2016 is the craze of the combination of information security behavior research and cognitive neuroscience. A total of six papers have been published, and 2017 has begun to decline, but it is still a continuous research topic.

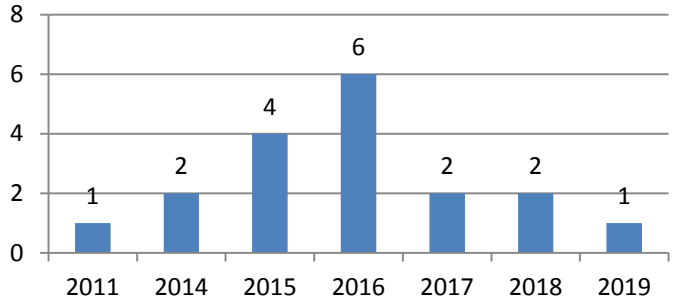

Figure 1. Number of published papers on neuro-information security in 2011-2019

In the study of cognitive neuroscience, there are many measurement tools support scholars to collect and measure data to obtain neurophysiological information from the brain, skin, and cells. Mainly include functional magnetic resonance imaging (fMRI), electroencephalography (EEG), eye tracking (ET), and functional near-infrared spectroscopy (fNIRS). Because of their different functions, in actual research, research the tools are usually selected according to the characteristics of the tool itself and the needs of the experiment. The more commonly used tools are fMRI, EEG and ET. The literature on cognitive safety neuroscience in 2011-2019 can be found in the use of cognitive tools by scholars, as shown in Figure 2.

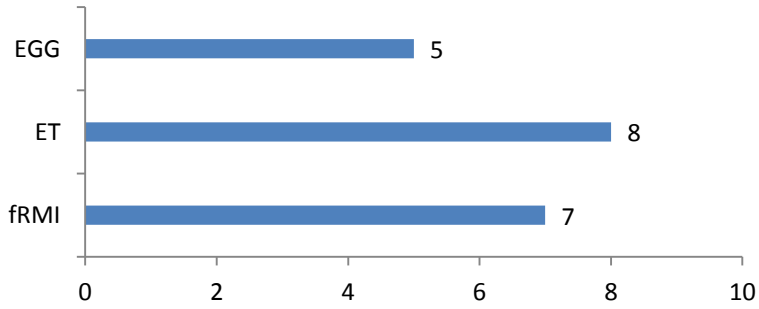

Figure 2. Number of uses of cognitive neural tools in information security research in 2011-2019

It can be found that in the current research, the frequency of use of ET, fMRI, and EEG is not much different, and the specific reason is the practicality and advantage of these tools. The application of each of the above cognitive neuroscience tools will be described below.

3. ET IN INFORMATION SECURITY BEHAVIOR RESEARCH

ET accurately measures eye position and eye movement, including eye gaze, pupil dilation, gaze time, and area of interest. ET is a highly regarded neuroscientific research tool. Its advantage is that it can measure human visual activity with high precision and time precision, and record the visual observation of the subject during the experiment sequence of activities. Using the eye tracker, the trajectory and hotspot of the eye movement can be drawn, and the temporal and spatial characteristics of the eye movement can be visually reflected. The line of sight of the subject and focus area is measured, as shown in Figure 3.

Figure 3. Heat map drawn by ET technology[4]

ET currently has a very wide range of research applications in the field of information systems. In terms of web design, eye movement research can optimize the web interface design through eye movement hotspots and trajectory maps that users pay attention to, to attract the attention of users. Except for web design, eye movement research has also progressed in the field of information systems such as human-computer interaction, advertising marketing, and reading.

Studies have shown that users are vulnerable to malicious information, such as phishing attacks, prompting users to install malware or accessing compromised websites. At the same time, users are often ignorant of software and system security warning light protection messages. Therefore, scholars in the field of information security have begun to study the user's visual focus on security warnings and other information to understand the user's attitude toward security warnings, as shown in Table 1.

Table 1. Research status of ET in information security behavior

Author	Topic	Participants	Amount	Conclusion
Bonnie B.Anderson[4-6]	Security warning ignored	College Students	102	Participants' attention to safety warnings decreases over time, and polymorphic warning styles reduce this compliance
Anthony Vance[7, 8]	Security warning ignored	College Students	62	Habituation is a factor that causes users to ignore information security warnings. Polymorphic warnings can reduce the impact of habituation.
Mohamed Alsharnouby[9]	Phishing message ignored	College Students	21	Viewers rarely pay attention to tips for dangerous information such as webpage fishing
G. Susanne Bahr[10]	Safety pop-up information	College Students	12	Users are annoying and annoying about the security pop-ups, thinking that they have interrupted their tasks, and more polite warnings will get more attention.
Aiping Xiong[11]	Web phishing	Adult	320	Even if the security information is highlighted in the domain bar, users still lack the ability to detect phishing information.

As shown in Table 1, the current research status of eye-moving technology in information security behavior focuses on the user's behavioral responses to security warnings, phishing messages, etc. Using ET technology, researchers can find warnings that users are facing information security tips. This helps explain the user's safety response behavior and guides safety warnings and pop-up design.

4. EEG IN INFORMATION SECURITY BEHAVIOR RESEARCH

When the human brain performs cognitive activities, the brain position will react differently, and the generated EEG signals will be different. With the strength and distribution of the electromagnetic signals in the brain of the subject, it can be inferred that the brain is cognitive the status of the activity process. Based on this principle, EEG is a psychological and physiological measure of the post-synaptic potential of the scalp. By placing the measured click tool at a specific location on the scalp, the vertebral neurons indicated from the cortex collect the sum of the cerebral cortical activity throughout the cognitive process, and then measure the position of each electrode with the fluctuation of the reference electrode. The situation is compared. In neuroscience tools, EEG has a high temporal resolution, can reflect the changes of the active process through the potential activity, and is presented in the form of waveforms and topographic maps, as shown in Figure 4.

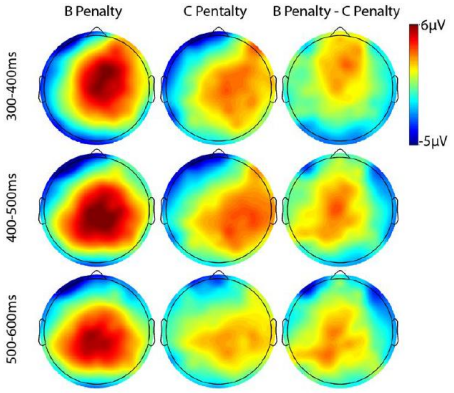

Figure 4. EEG topographic map[12]

The advantage of EEG is that the price cost is lower than other cognitive neural tools, and the experimental paradigm and operation are simple, which can increase the number of subjects and enhance the scientific rationality of data. Researchers use EEG to study users and can obtain EEG waveform data such as joy, frustration, and other cognitive states according to the brain reaction of the subjects to conduct more scientific research in the field of information systems. This brings a new research idea to the field of information security.

Table 2. Research Status of EEG in Information Security Behavior

Author	Topic	Participants	Amount	Conclusion
Dongmei Han[13]	Brain sensitivity to information security	Adult	12	The left hemisphere and beta waves are highly sensitive to safety messages and are a sign of risk assessment.
Anthony Vance[12]	security risk perception and behavior prediction	College Students	62	Self-reporting has a limited role in predicting information security behavior, and security behavior is affected by many factors.
Bridget Kirby[14]	Impact of security violation decisions	Adult	40	In information security violation decision-making, morality influences decision-making through neurological mechanisms, and rewards also influence security decisions.
Qing Hu[15, 16]	Security pop-up information	College Students	12	Self-control ability affects information security decision-making, high self-control ability, brain nerves are more active in security decision-making

It can be seen from Table 2 that the current research on EEG in information security behavior is mainly when the user makes safe behavior decision-making, and the brain nerve activity process fully reflects the user's cognitive process and decision-making behavior in information security behavior. It is the true response of the brain's neural mechanism, and the research methods such as self-reporting have deviations in this respect, which provides a basis for the use of neurocognitive tools in the field of information security.

5. FMRI IN INFORMATION SECURITY BEHAVIOR RESEARCH

Since the data of the EEG measurement tool reflects the activity history of the brain in the cognitive process, more emphasis is placed on the change in the time dimension during the research process, which has a strong temporal resolution, and in spatial resolution, Understanding the cognitive mechanisms of specific regions of the brain is measured by functional magnetic resonance imaging (fMRI). FMRI is a neuroimaging method that measures brain activity based on blood oxygen level-dependent (BOLD) contrast based on changes

in blood flow.

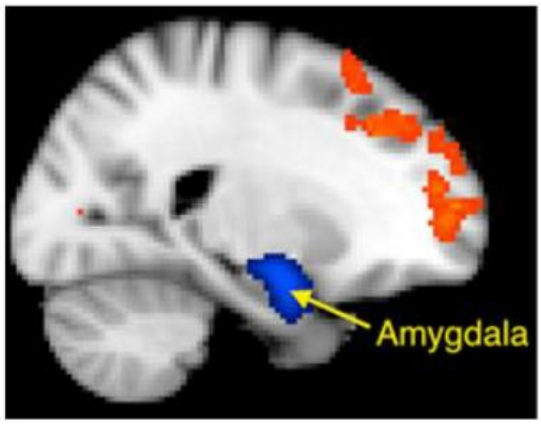

Figure 5. Image of brain activity under fMRI technology[17]

When a specific task activates a certain brain area, the energy consumption and oxygen supply to the area will increase significantly. By tracking the physiological parameters of blood supply oxygen or energy changes, you can know which part of the brain is more excited and active when the brain is engaged in specific tasks and tasks. As shown in Figure 5， the fMRI based on the blood oxygen level dependent (BOLD) signal can obtain a full brain functional activity image with a spatial resolution at the millimeter level in a few seconds.

Compared with EEG, fMRI is very demanding in experimental design and experimental environment, and the cost of its experiment is very expensive, but due to its non-invasive experimental methods, data analysis methods are the mature and high spatial resolution. Features are important tools for explaining the neural mechanisms and mental states of human behavior, especially when self-reporting is unreal for some reason. Therefore, the application value of fMRI in the field of information security will be very important. In past research, it is found that there is a deviation between the self-report and the actual behavior of the user's safety behavior. The reason for this deviation may be psychological factors and the environment. Causes and other reasons. Therefore, the use of neuroscience tools to study the brain cognitive response of users in safe behavior is an important focus of current information security, as shown in Table 3.

Table 3. Research Status of fMRI in Information Security Behavior

Author	Topic	Participants	Amount	Conclusion
Bonnie B .Anderson[18]	Security warning ignored	College Students	25	Static safety warnings are less active in the brain under habituation, and more polymorphic warnings
Anthony Vance[7, 8]	Security warning ignored	College Students	16	Polymorphic warnings can increase the user's attention to safety warnings while resisting the effects of habituation
Jeffrey L. Jenkins[19]	Security warning ignored	College Students	24	Dual-task interference is the cause of the user's security warning response capability, and reasonable limits on security warnings can improve responsiveness.
David Eargle[20]	The impact of emotions on safety warnings	College Students	23	Emotional warnings can further affect a user's ability to respond to security warnings
Merrill Warkentin[17]	Fear appeals response to security threats	College Students	17	Fear appeal theory can't attract users' reactions, and the method of focusing on threats is more attractive.
Ajaya Neupane[21]	Differentiate phishing and respond to security warnings	College Students	25	The brain has a highly functional connection to security testing, and brain activity is highly correlated between phishing and security warnings.

6. RESULTS

Although the investment in information security technology is increasing year by year, users are still the weakest link in information security. Therefore, the user's security behavior has become a topic of concern for information security scholars. In the existing research, most of the research data come from the subjective consciousness survey methods such as self-report, but it is difficult to obtain objective and real behavior data. But often the actual behavior under information security is a more important research variable than intent, and the intention is not directly related to behavior. Therefore, cognitive neuroscience provides new insights and perspectives for studying information security behaviors and cognition. It can be seen from Table 1, Table 2 and Table 3 that the research on information security behavior of cognitive neuroscience mainly focuses on the response behavior and neglect behavior of security warning, phishing webpage message and pop-up message. The participants are almost all college students, and the number is generally around 20. Future research can expand the research topic and scope by referring to the current research situation, such as using other occupations as subjects to discuss the applicability of current research.

When studying information security behaviors, the measurement of actual safety behavior data limits the development and verification of the theory. First, the target of the investigation report will deviate from the true behavioral response due to environmental, gender or self-efficacy, resulting in the final result. deviation. Second, although there is a strong relationship between the user's intention and the actual information security behavior, the measurement and use of behavioral data is still the most important method to consider behavior. Given these factors, neurocognitive science tools can help with information security behavior research as follows:

(1) ET. ET focuses on the visual tracking trajectory of the eye to record the visual focus points and motion trajectories of the user in the corresponding information security warnings, the development of information security decisions, etc., and the users recorded by the eye tracker perform safety behaviors. Data such as eye-gazing area and length of stay respond to the subconscious psychological cognitive response and preferences of users in information security behaviors and can guide the design and management of information security interface design and security alarms.

(2) EEG. EEG and ERP are an important basis for studying information security violations and response behaviors. In information security behavior research, the user's safe behavior is the real activity in the brain is a key factor to break with the current research, based on The self-reporting and investigation forms will be distorted because of the psychological factors of the respondents, but the EEG can use the waveform of the brain to truly reflect the real data of the user in the safe behavior, and can be used by the information security scholars in the user's safe behavior. Motivation and responsiveness research have brought important help.

(3) fMRI. In the field of information security, emotion and trust are very important factors. Many studies have pointed out that factors such as emotion and trust are important factors for users to influence the security behavior of users. Compared with EEG, fMRI can more clearly collect the active state of brain regions in user safety behaviors. It is an important tool to study topics such as user information security response behavior, irregular will, information security compliance, and security warning neglect.

Considering the advantages of fMRI in spatial resolution and the advantages of EEG in temporal resolution, as well as the visual tracking characteristics of ET on the ocular nerve. Combining multiple neuroscience tools to measure and analyze is a key idea for future research on information security behaviors and cognitive processes.

7. CONCLUSION

Neurocognitive science has opened up a new paradigm for studying information security and has formed a certain academic influence in the field of information security research. The data obtained by neuroscience tools

is based on subjective physiological phenomena and other scale data, which solves the subjective influence of survey access, observation and self-report in previous information security research. By searching for the laws and relationships of these data, researchers can more accurately capture the influencing factors and laws under the phenomena and information security behaviors. It is the information security compliance, information security violations, security neglect and in the future information security research. An important reference for the study of safety behaviors influenced by factors such as trust and emotion.

This paper reviews the research status of cognitive neuroscience in the field of information security. By using the neurocognitive science tools ET, EEG and fMRI as clues to analyze information security research, it is found that the application of neuroscience in the research of information security behavior has gradually attracted the attention of researchers. The reason is that cognitive neuroscience can mine data such as physiological signals and behaviors, and a more subjective and thorough explanation of the hidden factors that affect the safe behavior of users' information. By summarizing the existing research, we can find that the main hotspot of current neuroscience research on information security behavior is to reveal the user's behavior when warning messages such as security warnings and phishing information and analyze the neural mechanism of users ignoring and responding to security warnings. The active state of the brain at the time of behavior provides a more realistic study of information security behavior research. However, it can also be found that the current themes of neuroscience in the field of information security are relatively simple. Through the summary of the current field in this paper, follow-up research can be extended on the theme of current information security behavior, with the advantages of neurocognitive tools in data collection, revealing the objective facts of more information security behaviors.

The shortcoming of this paper is that it only studies and summarizes the mainstream tools in the field of current neural information systems. It does not make a statement about other cognitive neural tools. The next step is to make cross-applications in the field of cognitive neuroscience tools and information security. A more comprehensive summary and research.

ACKNOWLEDGEMENT

This research has been funded by Humanities and Social Science Research Projects in Ministry of Education of China (No. 16YJA630056), National Science Foundation of China (Nos. 71331003, 71471080, 71471078, and 71471079).

REFERENCES

[1] Riedl R, Banker R D, Benbasat I, et al. (2010). On the Foundations of NeuroIS: Reflections on the Gmunden Retreat 2009[J]. Communications of the Association for Information Systems, 27: 243-264.

[2] Riedl R, Fischer T, Leger P-M. (2018)A Decade of NeuroIS Research: Status Quo, Challenges, and Future Directions[C]38th International Conference on Information Systems: Transforming Society with Digital Innovation, ICIS 2017, December 10, 2017 - December 13, 2017. Seoul, Korea, Republic of: Association for Information Systems, 2018. Bibigo; Dongwon F and B; et al.; Mario Outlet; MIT CISR; Seoul Tourism Organization.

[3] Crossler R, Johnston A, Lowry P, et al. (2013). Future directions for behavioral information security research[J]. Computers & Security, 32(C): 90-101.

[4] Anderson B B, Jenkins J L, Vance A, et al. (2016). Your memory is working against you: How eye tracking and memory explain habituation to security warnings[J]. Decision Support Systems, 92: 3-13.

[5] Anderson B B, Vance A, Kirwan C B, et al. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study[J]. European Journal of Information Systems, 25(4): 364-390.

[6] Anderson B B, Bjornn D, Jenkins J, et al. (2018). Improving security message adherence through improved

comprehension: Neural and behavioral insights[C] 24th Americas Conference on Information Systems 2018. New Orleans, LA, United states: Association for Information Systems, 2018. Louisiana State University (LSU).

[7] Vance A, Kirwan B, Bjornn D, et al. (2017) . What do we really know about how habituation to warnings occurs over time? A longitudinal fMRI study of habituation and polymorphic warnings[C]2017 ACM SIGCHI Conference on Human Factors in Computing Systems. Denver, CO, United states: Association for Computing Machinery, 2215-2227.

[8] Vance A, Jenkins J L, Anderson B B, et al. (2018). Tuning out security warning: A longitudinal examination of habituation through fMRI, eye track, and field experiments[J]. MIS Quarterly, 42(2): 355-A15.

[9] Alsharnouby M, Alaca F, Chiasson S. (2015). Why phishing still works: User strategies for combating phishing attacks[J]. International Journal of Human-Computer Studies, 82: 69-82.

[10] Bahr G S, Ford R A. (2011). How and why pop-ups don't work: Pop-up prompted eye movements, user affect and decision making[J]. Computers in Human Behavior, 27(2): 776-783.

[11] Xiong A, Proctor R W, Yang W, et al. (2017). Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages?[J]. Human Factors, 59(4): 640-660.

[12] Vance A, Brinton Anderson B, Brock Kirwan C, et al. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG)[J]. Journal of the Association for Information Systems, 15(10): 679-722.

[13] Han D, Dai Y, Han T, et al. (2015). Explore Awareness of Information Security: Insights from Cognitive Neuromechanism[J]. Computational Intelligence & Neuroscience, 2015: 1-8.

[14 Kirby B, Malley K, West R. (2019). Neural Activity Related to Information Security Decision Making: Effects of Who Is Rewarded and When the Reward Is Received[C]//F.D. Davis, R. Riedl, J. vom Brocke, et al. Information Systems and Neuroscience. Cham: Springer International Publishing, 19-27.

[15] Hu Q, West R, Smarandescu L, et al. (2014). Why Individuals Commit Information Security Violations: Neural Correlates of Decision Processes and Self-Control[C]Hawaii International Conference on System Sciences.

[16] Hu Q, West R, Smarandescu L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective[J]. Journal of management information systems, 31(4): 6-48.

[17] Warkentin M, Walden E, Johnston A C, et al. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination[J]. Journal of the Association for Information Systems, 17(3): 194-215.

[18] Anderson B B, Vance A, Kirwan C B, et al. (2016). From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It[J]. Journal of management information systems, 33(3): 713-743.

[19] Jenkins J L, Anderson B B, Vance A, et al. (2016). More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable[J]. Information Systems Research, 27(4): 880-896.

[20] Eargle D, Kirwan C B, Galletta D, et al. (2016). Integrating facial cues of threat into security warnings-an fMRI and field study[C]22nd Americas Conference on Information Systems: Surfing the IT Innovation Wave, AMCIS.

[21] Neupane A, Saxena N, Maximo J O, et al. (2016). Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings[J]. IEEE Transactions on Information Forensics and Security, 11(9): 1970-1983.