IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

# AI-Enhanced Cybersecurity Training: Learning Analytics in Action

**Ravi Chourasia**
Lead Software Engineer

**Abstract:** *Cybersecurity is growing increasingly intricate due to the rapid expansion of interconnected systems and the global landscape of threats. To address these challenges effectively, a proficient cybersecurity workforce capable of making complex decisions in the ever-changing cyberspace is essential. While Artificial Intelligence (AI) is being quickly integrated into cybersecurity operations, it is crucial to comprehend the foundational learning theory and ecosystems to adequately train human operators and AI-assisted cyber defense teams. Cybersecurity exercises (CSXs) serve as popular instructional tools for cyber preparedness. Nevertheless, the utilization of learning analytics (LA) techniques and AI-driven approaches in exercise development and implementation is still nascent. We advocate for a comprehensive model of human-AI interaction within the context of LA and CSX. This model unifies aspects of human-AI interaction, cyber ranges, cybersecurity practices, LA tools, multimodal learning analytics, exercise life cycles, and pedagogical strategies. We also explore the potential and obstacles for implementing LA and AI in cybersecurity training. By examining the role of AI through a lens of learning, instruction, and administration in cybersecurity training, particularly within exercises, we seek to prompt further discourse on the future of collaboration between humans and AI and how to enhance cybersecurity training through innovative LA and AI capabilities.*

**Keywords:** E-Commerce, Information, Choices, Precise, Transactions, Intuitive

## I. INTRODUCTION

Our society's increasing reliance on digital solutions and technological advancements poses current and future risks in cyberspace. The complexity of cybersecurity is on the rise, despite the automation of many cybersecurity tasks and the use of more Artificial Intelligence (AI) tools. Human intervention remains crucial for critically evaluating and identifying errors in tasks performed by AI agents. Collaborative efforts are essential to effectively address these challenges. A neutral and evidence-based comprehension of the collaboration between human-AI cyber defense teams and methods for preparing for this forthcoming reality is of utmost importance.

The training of future human operators in human-AI cyber defense teams must tackle various challenges such as determining the necessary knowledge and skills to prevent the degradation of traditional cybersecurity skills, creating practical learning scenarios, and assessing the efficacy of different teaching approaches with a focus on experiential learning.

Effective training for future human operators entails three key components: 1) educating individuals on how to cooperate with AI, 2) empowering human operators to detect potential AI manipulation or threats, and 3) utilizing AI to enhance and evaluate their learning through efficient learning analytics (LA).

Consequently, cybersecurity training should address the difficulties and leverage the advantages presented by LA and AI to keep pace with rapid technological advancements. In the realm of cybersecurity education and training, Cyber Security Exercises (CSXs) like blue/red, simulation, tabletop, and capture-the-flag exercises are popular methods for enhancing cyber readiness. Conducting such exercises in the age of AI necessitates a change in mindset and the adoption of new methodologies and theories from the perspectives of instructors and organizers.

The endeavor to provide students with a thorough and interdisciplinary grasp of cybersecurity principles and practices for safeguarding digital systems and data in the AI era raises numerous questions in the field of cybersecurity education and training. Nonetheless, formulating and applying relevant discipline-specific theories can be demanding, and oftentimes, it is simpler to rely on established theories. Establishing a solid base and a shared comprehension of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

pertinent discipline-specific theories or building upon established, widely accepted theories offers guidance and aids in the evolution of the discipline.

## II. PREVIOUS WORK

Collaboration between humans and artificial intelligence (AI) systems has been an area of extensive research, especially in contexts such as zero-shot coordination (ZSC) and cybersecurity training. The challenge lies in fostering seamless integration between human and AI agents to achieve shared goals in dynamic, unfamiliar scenarios.

### Zero-Shot Coordination and the COLE Framework

Zero-shot coordination (ZSC) involves training AI agents to collaborate effectively with previously unseen partners, including humans and other AI systems. Traditional self-play (SP) methods, while successful in optimizing rewards within fixed populations, often fall short when exposed to unfamiliar strategies due to their tendency to develop rigid conventions (e.g., Tesauro, 1994; Carroll et al., 2020). Recent advancements, such as the Cooperative Open-ended Learning (COLE) framework, have addressed this limitation by leveraging Graphic-Form Games (GFGs) and Preference GFGs (P-GFGs) to evaluate and optimize cooperative capacity. Algorithms like COLESV and COLER have shown promise in overcoming cooperative incompatibility, as demonstrated in experimental environments like Overcooked and validated through extensive human-AI studies.

### Cybersecurity Training and Learning Analytics

In cybersecurity education, Cybersecurity Exercises (CSXs) such as red/blue team simulations and capture-the-flag events are well-established methods for enhancing cyber-readiness. The integration of learning analytics (LA) into CSXs has enabled data-driven insights into participant behavior, improving the efficacy of training. However, the incorporation of AI into LA frameworks remains in its infancy. Existing platforms primarily employ manual analysis methods, focusing on descriptive statistics and visual feedback. Despite progress in areas like multimodal analytics and real-time feedback mechanisms, challenges persist in adapting AI-driven LA tools to measure trust, adaptability, and collaboration within human-AI teams.

### Bridging the Gap

While ZSC research has primarily concentrated on optimizing cooperative algorithms in controlled environments, cybersecurity training has emphasized experiential learning within structured scenarios. Bridging these domains involves addressing the unique challenges of human-AI interaction in high-stakes, real-world contexts. This includes designing adaptive learning environments, fostering trust in AI systems, and developing metrics to evaluate collaborative fluency and decision-making.

## III. NATURAL LANGUAGE PROCESSING

While Zero-Shot Coordination (ZSC) research has primarily focused on optimizing cooperative algorithms within controlled environments, such as simulated games or predefined scenarios, cybersecurity training emphasizes experiential learning in structured and dynamic scenarios. This dichotomy presents unique opportunities and challenges when aiming to integrate these domains. Bridging ZSC research and cybersecurity training requires addressing several critical aspects to ensure effective human-AI collaboration in high-stakes, real-world environments:

### Designing Adaptive Learning Environments

Adaptive learning environments tailored to both human and AI participants are essential for addressing the dynamic nature of cybersecurity scenarios. Unlike ZSC algorithms that rely on pre-defined objectives and environments, cybersecurity contexts demand real-time adaptability. Cyberattacks evolve rapidly, requiring both humans and AI to respond dynamically to novel threats. Leveraging adaptive AI, which can modify its strategies based on human behavior and situational context, ensures that collaborative teams are better equipped to handle unpredictable scenarios. These environments must also provide iterative learning cycles, where both humans and AI agents can learn from their actions and refine their strategies collaboratively.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

**Fostering Trust in AI Systems**

Trust is a cornerstone of successful human-AI collaboration, particularly in high-risk domains like cybersecurity. ZSC research often assumes that AI agents operate optimally in a team setting; however, real-world applications reveal discrepancies in human understanding and acceptance of AI decisions. Fostering trust involves creating AI systems that are not only transparent in their decision-making processes but also capable of explaining their reasoning in ways that are intuitive to human collaborators. This is particularly important in cybersecurity, where a lack of trust in AI recommendations can lead to delays in critical decisions or over-reliance on flawed outputs. Strategies to foster trust include incorporating explainable AI (XAI) techniques and conducting training exercises that build human confidence in AI capabilities.

**Developing Metrics to Evaluate Collaboration**

One of the primary challenges in bridging ZSC and cybersecurity training lies in developing robust metrics to evaluate the effectiveness of human-AI collaboration. Metrics must go beyond traditional performance indicators like task completion time or accuracy. Instead, they should encompass nuanced aspects of collaboration, such as team fluency, mutual understanding, and adaptability. For example, in ZSC, metrics often focus on cooperative fluency and coordination efficiency within a game environment. In cybersecurity, these metrics must be expanded to include the human perception of AI reliability, the ability of AI to adapt to human strategies, and the overall effectiveness of the team in mitigating complex cyber threats.

**Addressing the Challenges of High-Stakes Contexts**

Real-world cybersecurity scenarios involve high stakes, where failures can lead to significant financial losses, reputational damage, or even threats to national security. Unlike ZSC research that often operates within simulated, low-risk environments, cybersecurity training must prepare teams for scenarios where errors have severe consequences. This necessitates the development of training environments that simulate the pressure, unpredictability, and complexity of real-world cyber incidents. Furthermore, these environments must allow for iterative learning and debriefing to identify gaps in collaboration and refine strategies.

**Integrating Human and AI Strengths**

A successful bridge between ZSC and cybersecurity training also requires leveraging the complementary strengths of humans and AI. Humans excel in creative problem-solving, ethical decision-making, and interpreting context. On the other hand, AI excels in processing vast amounts of data, identifying patterns, and executing repetitive tasks efficiently. Training environments must be designed to capitalize on these strengths, ensuring that human-AI teams operate as cohesive units where each member contributes optimally to the shared objective.

## IV. FRAMEWORK: DESIGNING ADAPTIVE LEARNING ENVIRONMENTS

**Study Overview**

Adaptive Learning Environments (ALEs) must dynamically adjust to the evolving needs of human-AI teams, leveraging multimodal data and adaptive algorithms to ensure continuous improvement. Below is a design blueprint with key components:

**Components of Adaptive Learning Environments**

- **Data Input Layer**: Collects real-time data from human and AI interactions.
- **Multimodal Inputs**: Clickstream data, biometrics, task performance metrics, and natural language interactions.
- **Adaptive Engine**: Processes inputs to adjust tasks, difficulty, or AI behavior dynamically.
- Composed of machine learning models and rule-based systems.
- **Feedback Mechanism**: Provides actionable insights to both humans and AI agents.
- **Evaluation Metrics**: Quantifies the success of adaptations (e.g., trust levels, task efficiency).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

**Algorithm: Adaptive Task Allocation (ATA)**
**Goal**: Adjust task complexity based on the performance of human-AI teams to maintain optimal learning conditions.

**Steps:**
**Initialization**:
Define task complexity levels T={T1,T2,...,Tn}
Set initial complexity Tinit based on pre-assessment.
**Real-Time Monitoring**:
Monitor task performance metrics:
**Human Response Time (HRT)**: Rt
**AI Confidence Score (AICS)**: Ct
**Error Rate (ER)**: Et
Multimodal input vectors: Xt={Rt,Ct,Et}
**Adaptation Logic**:
Compute the **adaptation score**: St=w1·Rt+w2·Ct+w3·(1−Et)where w1,w2,w3 are weight parameters.
Define thresholds for adaptation

If $S_t < \alpha$, decrease complexity to $T_{t-1}$.

If $S_t > \beta$, increase complexity to $T_{t+1}$.

**Update Task Environment**:
Adjust task Tt based on St.
**Feedback Loop**:
Provide tailored feedback Ft to participants and AI: Ft={human performance insights,AI strategy optimization}
**Algorithm: Adaptive Role Allocation (ARA)**
**Goal: Dynamically assign roles to human and AI agents based on capabilities and workload.**
**Steps:**
**Initialization**:
Define roles R={R1,R2,...,Rm}.
Assign initial roles based on skill scores Hs,Asfor humans and AI.
**Real-Time Role Evaluation**:
Calculate workload balance W:

$$W = \frac{\sum_{i=1}^{m} \text{Task Load}_i}{\sum_{j=1}^{n} \text{Capacity}_j}$$

where m is the number of tasks, and n is the number of team members.
Evaluate task success probability Pt.

$$P_t = \frac{H_s}{H_s + A_s}.$$

**Adaptation Logic**:
If W>γ, reallocate tasks to balance the workload.
Assign tasks based on success probability Pt:
Assign tasks with Pt>0.5 to humans.
Assign tasks with Pt≤0.5to AI.

**Test Results and Discussion**
To validate the effectiveness of the proposed Adaptive Learning Environment (ALE) framework, we conducted a controlled experiment simulating human-AI collaboration in dynamic and high-stakes scenarios. The experiment aimed

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

to assess the system's adaptability, efficiency, and its ability to foster trust and collaboration between human participants and AI agents.

## V. EXPERIMENT DESIGN

**Objective:** To evaluate the impact of ALE on improving task efficiency, team fluency, trust, and adaptation in real-time collaborative environments.

**Participants:**

50 human participants with varying expertise in cybersecurity and team-based problem-solving.

AI agents trained using the Cooperative Open-ended Learning (COLE) framework, enhanced with adaptive algorithms for task and role allocation.

**Scenarios:**

**1. Cybersecurity Exercises (CSXs):**

Participants engaged in simulated red/blue team cybersecurity scenarios, designed to emulate real-world threat landscapes. Tasks included:

Identifying and mitigating cyberattacks such as phishing attempts, Distributed Denial of Service (DDoS) attacks, and ransomware incidents.

Securing critical infrastructure components, including firewalls, network nodes, and databases.

Collaboratively responding to advanced persistent threats (APTs), requiring dynamic decision-making and role-based teamwork.

These scenarios were executed in a controlled cyber range environment equipped with AI-driven threat detection and response tools. The exercises were designed to test adaptability, trust, and coordination under realistic cyber crisis conditions.

**2. Collaborative Gaming (Overcooked):**

In parallel, participants worked with AI agents in a cooperative gaming scenario, "Overcooked," which required synchronization, task-sharing, and adaptability to complete time-sensitive objectives.

**Metrics Evaluated:**

**Task Efficiency (TE):** The ratio of optimal task completion time to actual completion time.

**Team Fluency (TF):** Smoothness of interactions measured by the number of task interruptions and redundant actions.

**Trust Index (TI):** Human trust in AI, measured through post-task surveys and in-task reliance on AI suggestions.

**Adaptation Score (AS):** Effectiveness of the ALE framework in dynamically adjusting task difficulty and role assignments.

**Key Results**

**1. Task Efficiency (TE):**

**Baseline AI:** Average TE was 0.68, indicating significant delays in task completion due to static task structures and a lack of adaptability.

**Adaptive AI (ALE):** Average TE improved to 0.85, a 25% increase, as tasks were dynamically adjusted to match human skill levels and AI capabilities.

In the cybersecurity scenario, the adaptive framework reduced the time required to identify and neutralize threats by dynamically reallocating tasks between human and AI team members based on their individual performance.

**2. Team Fluency (TF):**

**Baseline AI:** TF was 0.72, with frequent miscommunication and overlapping actions between human participants and AI agents.

**Adaptive AI (ALE):** TF increased to 0.91, a 26% improvement.

In red/blue team exercises, task reassignment ensured smooth transitions between detection, containment, and mitigation phases, reducing errors and improving overall team synchronization.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

**3. Trust Index (TI):**

**Baseline AI:** Participants exhibited a trust index of 0.65, often hesitating to rely on AI recommendations.

**Adaptive AI (ALE):** Trust index improved to 0.81, as participants expressed confidence in the AI's transparency and decision-making processes.

Trust was particularly evident in scenarios where the AI explained its rationale for detecting advanced persistent threats, which encouraged human participants to act on its recommendations promptly.

**4. Adaptation Score (AS):**

The ALE framework achieved an average AS of 0.88. Approximately 90% of tasks were dynamically adjusted to participant performance within three iterations, maintaining engagement without overwhelming users.

**Insights from the Cybersecurity Scenario**

The cybersecurity use case underscored the real-world applicability of the ALE framework in high-stakes environments. Participants highlighted several key advantages:

- **Dynamic Threat Allocation:** By leveraging real-time performance metrics, the ALE framework reassigned complex threat mitigation tasks to AI while allowing human participants to focus on strategic decisions.
- **Improved Decision-Making:** Multimodal analytics provided valuable insights into participant behavior, enabling the AI to offer personalized suggestions and prioritize critical threats.
- **Building Resilience:** The simulated APT scenarios forced human-AI teams to adapt to evolving threats, fostering resilience and improving overall system performance.

## VI. FUTURE WORK

Building on the promising results of our Adaptive Learning Environment (ALE) framework, several avenues for future research and development have been identified to enhance its capabilities and expand its applicability. Below are key directions for future work:

**1. Scaling to Complex Real-World Scenarios**

While the current experiments demonstrated the effectiveness of ALE in controlled environments, future work will focus on scaling the system to address more complex, real-world scenarios, such as:

- **Critical Infrastructure Protection:** Applying ALE to secure energy grids, healthcare systems, and transportation networks from sophisticated cyber threats.
- **Cross-Domain Applications:** Extending the framework to fields like disaster response, autonomous vehicle operations, and smart city management.
- **Objective:** Ensure that ALE can handle the dynamic, multi-faceted challenges of larger, more interconnected systems.

## VII. CONCLUSION

The results of the experiment demonstrate that the Adaptive Learning Environment (ALE) framework effectively enhances human-AI collaboration by improving efficiency, fluency, and trust. The dynamic adjustments in task allocation, particularly in the cybersecurity use case, proved invaluable in high-pressure situations, reducing response times and enhancing collaborative outcomes. These findings highlight the potential of ALE to transform cybersecurity training and operations, preparing teams for the challenges of real-world threats.

Future work will explore scaling the system to larger, more complex scenarios, incorporating additional threat types, and refining the multimodal analytics to support even greater levels of adaptability and collaboration.

## REFERENCES

[1] K. Maennel, R. Ottis, and O. Maennel, “Improving and measuring learning effectiveness at cyber defense exercises,” in Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22, pp. 123–138, Springer, 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

[2] C. Szabo, N. Falkner, A. Petersen, H. Bort, K. Cunningham, P. Don- aldson, A. Hellas, J. Robinson, and J. Sheard, "Review and use of learning theories within computer science education research: Primer for researchers and practitioners," in Proceedings of the working group reports on innovation and technology in computer science education, pp. 89–109, 2019.

[3] B. F. Mon, A. Wasfi, M. Hayajneh, and A. Slim, "A study on role of artificial intelligence in education," in 2023 International Con- ference on Computing, Electronics & Communications Engineering (iCCECE), pp. 133–138, IEEE, 2023.

[4] J. Jacob, M. Peters, and T. A. Yang, "Interdisciplinary cybersecurity: Rethinking the approach and the process," in National Cyber Summit (NCS) Research Track, pp. 61–74, Springer, 2020.

[5] E. Berki, J. Valtanen, S. Chaudhary, and L. Li, "The need for multi- disciplinary approaches and multi-level knowledge for cybersecurity professionals," in Multidisciplinary perspectives on human capital and information technology professionals, pp. 72–94, IGI Global, 2018.

[6] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou, "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline," in Proceedings companion of the 23rd annual ACM conference on innovation and technology in computer science education, pp. 36– 54, 2018.

[7] C. E. Wilson, "Cybersecurity education: The emergence of an accredited academic discipline?," in Journal of The Colloquium for Information Systems Security Education, vol. 2-1, pp. 13–13, 2014.

[8] High-Level Expert Group on Artificial Intelligence (AI HLEG), "A definition of ai: Main capabilities and scientific disciplines," tech. rep., European Commission, 2018.

[9] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 97, p. 101804, 2023.

[10] S. Samoili, M. L. Cobo, E. Gómez, G. De Prato, F. Martínez-Plumed, and B. Delipetrev, "Ai watch. defining artificial intelligence. towards an operational definition and taxonomy of artificial intelligence," JRC Research Reports JRC118163, 2020.

[11] W. Cai, L. Pasquale, K. Ramkumar, J. McCarthy, B. Nuseibeh, and G. Doherty, "Human-ai collaboration for sustainable security: Opportunities and challenges," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2023.

[12] A. Chowdhury, H. Nguyen, D. Ashenden, and G. Pogrebna, "Poster: A teacher-student with human feedback model for human-ai collab- oration in cybersecurity," in Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, pp. 1040– 1042, 2023.

[13] A. I. Hauptman, B. G. Schelble, N. J. McNeese, and K. C. Madathil, "Adapt and overcome: Perceptions of adaptive autonomous agents for human-ai teaming," Computers in Human Behavior, vol. 138, p. 107451, 2023.

[14] K. Maennel, "Learning analytics perspective: Evidencing learning from digital datasets in cybersecurity exercises," in 2020 IEEE Eu- ropean symposium on security and privacy workshops (EuroS&PW), pp. 27–36, IEEE, 2020.

[15] R. Beuran, J. Vykopal, D. Belajová, P. Čeleda, Y. Tan, and Y. Shin- oda, "Capability assessment methodology and comparative analysis of cybersecurity training platforms," Computers & Security, vol. 128, 2023.

[16] M. Albaladejo-González, S. Strukova, J. A. Ruipérez-Valiente, and F. GómezMármol, "Exploring the affordances of multimodal data to improve cybersecurity training with cyber range environments," Ediciones de la Universidad de Castilla-La Mancha: Cuenca, Spain, 2021.

379

[17] V. Švábenskỳ, J. Vykopal, P. Čeleda, and J. Dovjak, "Automated feedback for participants of hands-on cybersecurity training," Edu- cation and Information Technologies, pp. 1–30, 2023.

[18] V. Švábenskỳ, J. Vykopal, P. Čeleda, and L. Kraus, "Applications of educational data mining and learning analytics on data from cybersecurity training," Education and Information Technologies, vol. 27, no. 9, pp. 12179–12212, 2022.

[19] J. Vykopal, P. Seda, V. Švábenskỳ, and P. Čeleda, "Smart environ- ment for adaptive learning of cybersecurity skills," IEEE Transac- tions on Learning Technologies, vol. 16, no. 3, pp. 443–456, 2022.

[20] M. M. Yamin and B. Katt, "Modeling and executing cyber security exercise scenarios in cyber ranges," Computers & Security, vol. 116, p. 102635, 2022.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

[21] A. Uzal, L. Tobarra, A. Utrilla, A. Robles-Gómez, R. P. Vargas, and R. Hernández, "Tracking the students' learning behavior for cybersecurity scenarios.," in LASI-SPAIN, pp. 143–155, 2020.
[22] R. Pandey, B. Bannan, and H. Purohit, "Citizenhelper-training: Ai- infused system for multimodal analytics to assist training exer- cise debriefs at emergency services," in ISCRAM 2020 conference proceedings–17th international conference on information systems for crisis response and management, 2020.
[23] K. M. Eisenhardt, "Building theories from case study research," Academy of management review, vol. 14, no. 4, pp. 532–550, 1989.