SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 01 (2025), pp. 20-26
Research Article
doi: https://doi.org/0.70710/sitj.v2i1.28

Kufal Symbiosis: Collaboration of Artificial Intelligence and Terrorist Organizations

Wahyu Jati Arya Guna[1,a,*]

[1]Sekolah Tinggi Intelijen Negara, Bogor
[a]wahyujati.ag@gmail.com
*Corresponding author

Article Info
Received: 16-Dec-2024
Revised: 29-Jan-2025
Accepted: 30-Jan-2025

Keywords
AI and Terrorist; Cyber Terrorism; Cyberattacks by Terrorist; Potential Scenarios

Abstract
This paper delves into the phenomenon of "kufal symbiosis," which refers to the collaboration between artificial intelligence (AI) and terrorist organizations. It highlights AI's potential to enhance the efficiency of terrorist operations. While AI can be used to recruit new members and plan more sophisticated attacks, security agencies face challenges in adapting this technology to counter terrorism effectively. This paper discussed the crucial need to strike a balance between individual privacy and national security, as well as the difficulties of managing large-scale data with limited resources. Additionally, the use of technology such as deepfakes and botnets by terrorist organizations might lead to confusion and intensify the impact of their attacks. The discussion also addresses cyberattacks on smart cities, exposing the vulnerabilities in infrastructure to cyber threats. In conclusion, while AI enhances the efficiency of terrorist operations, it also equips security agencies to prevent such threats despite the ongoing struggle to balance privacy and security.

1. Introduction

The rapid development of artificial intelligence (AI) has profoundly transformed various aspects of human life. At the same time, AI offers excellent potential to improve efficiency, productivity, and quality of life. However, this technology can also be exploited for malicious purposes, particularly by extremist and terrorist organizations. The collaboration between artificial intelligence and terrorist organizations, which in this context is referred to as "*kufal* symbiosis", is an asymmetric interaction that represents an increasingly concerning phenomenon. Terrorist organizations can leverage the capabilities of AI to enhance their operations, ranging from recruiting new members to planning more advanced and less detectable attacks.

AI and terrorism are interconnected in various ways. In the context of terrorism, AI poses new challenges to national security, and both terrorist organizations and government agencies seek to exploit this technology for their purposes. AI and machine learning techniques have become crucial in understanding and predicting terrorist operations, although issues related to data accuracy and complexity persist (Saidi & Trabelsi, 2022). In general, while the advancement of AI offers impressive advantages, it also introduces new challenges that demand careful consideration from both the public and the government (Bazarkina & Pashentsev, 2019). Consequently, a thorough and nuanced understanding is necessary to anticipate the impact of the collaboration between AI and terrorism.

2. Literature Review

2.1. Kufal Symbiosis

Kufal symbiosis is a broader term that includes various types of interactions, including mutualism, but it can also extend to more complex interactions. In this context, *Kufal* symbiosis refers to mutually beneficial relationships that are not necessarily limited to two species. For instance, in social or technological settings, *kufal* symbiosis can describe collaborations between humans and artificial intelligence (AI). In such collaborations, humans benefit from AI's efficiency and analytical capabilities, while AI obtains data and context from these interactions, thereby enhancing its performance (Safira et al., 2017; Theowidavitya et al., 2019). In this case, *kufal* symbiosis involves interactions that may extend beyond two entities.

2.2. Artificial Intelligence

Artificial Intelligence is a branch of computer science focused on creating systems or technologies that can perform tasks typically requiring human intelligence. These tasks include learning, understanding language, recognizing patterns, and reasoning. AI is generally divided into two main categories, which are, Weak AI or Narrow AI and Strong AI or General AI (Bazarkina & Pashentsev, 2020). Weak AI is specifically designed to perform specific tasks exceptionally well. Examples include programs that can play chess, provide purchase recommendations, or predict weather forecasts. Weak AI lacks self-awareness and does not understand anything beyond its programmed functions. Currently, all existing AI is classified as Weak AI, also known as Narrow AI (Bazarkina & Pashentsev, 2019). In contrast, General AI refers to systems that can think, learn, and apply knowledge in various ways similar to human behavior. Strong AI is envisioned to perform intelligent operations across multiple domains. While Strong AI remains a theoretical concept and has not yet been realized, experts believe its development will progress more rapidly and effectively than previous generations of technology (Bazarkina & Pashentsev, 2019). The key distinction between Narrow and General AI lies in the range and complexity of tasks they can handle.

Managing AI as technology raises challenges requiring adequate governance, with the state serving a pivotal role in ensuring that AI regulation is consistent with public good and moral values (Papyshev & Yarime, 2023). In such circumstances, AI plays a vital role in the handling of such intense information, which facilitates more excellent system analysis and increases the system's ability to respond to changing environments (Munir et al., 2021). After the AI integration, surveillance systems can add more value and assist in more excellent reliability in the monitoring process (Munir et al., 2021). AI technology, in this respect, is compelling, and its impact on users is likely substantial. It can be viewed as a double-edged sword: for the good or the worst, it all depends on how one plans to use it.

2.3. Terrorism

Terrorism is defined as "the creation and exploitation of fear through violence or the threat of violence in an effort to achieve political change" (Uddin et al., 2020). This mainly targets civilians and involves different forms of violence, such as bombings, shootings, and kidnappings. Terrorism can also be understood as an attempt to create fear among the general public, frequently linked to aspirations to control or maintain control over a specific territory (Radil & Castan Pinos, 2022). In the context of cyberterrorism, it also includes the use of information and communication technology to support terrorist operations, such as recruitment, communication, and fundraising. However, violent acts carried out directly through the internet are still considered a more hypothetical threat (Broeders et al., 2023). In the context of ISIS, terrorism is characterized by the use of an extreme ideology that views violence as an acceptable method to reach its objectives, such as the creation of a caliphate and the enforcement of a radical interpretation of Islamic law (Martineau et al., 2022).

Terrorism is defined as an act in which a non-state entity uses physical force or threats to compel its demands through fear onto others, with the aim of advancing its political, economic, religious, or social agenda (Khan et al., 2023). Terrorism can disrupt national stability, peace, and international cooperation and hinder economic development and the protection of human rights (Campedelli et al., 2021). In the context of cyber terrorism, it can involve an attack conducted through information technology that destroys

critical infrastructures or instills fear in the public (Tehrani et al., 2013). It could also pertain to terrorism involved in cyberattacks, specifically with the increased utilization of the IoT that will be leveraged to conduct worse and other types of attacks (Tzezana, 2017). Terrorism can lead to a reduction in foreign investment, slower economic growth, and impacting social sectors such as health (Ouedraogo et al., 2023).

3. Method

This research uses a qualitative approach with a literature study method. The qualitative approach is ideal for exploring complex issues in depth, such as how artificial intelligence could amplify terrorism threats. The literature study method was selected because it focuses on collecting data from diverse written sources, including scientific journals, books, articles, and other documents. In addition to collecting data, the literature review involves a thorough analysis of the collected information to uncover patterns, connections, and conclusions related to the research topic.

4. Result and Discussion

4.1. The Collaboration of Artificial Intelligent and Terrorism

In the context of collaboration between artificial intelligence (AI) and terrorist organizations, *kufal* symbiosis can be understood as a mutually beneficial interaction between two distinct entities in which AI is utilized to support or enhance terrorist operations. In this case, AI serves as a tool that improves the efficiency and effectiveness of terrorist organizations' operations, whether in planning, execution, or propaganda. For instance, terrorist organizations may leverage AI technology to analyze extensive scale data, plan attacks, and spread their ideology through social media in a more targeted and effective way (Nugrahajati, 2024). The involvement of artificial intelligence (AI) in the world of terrorism has significantly increased both the complexity and scale of the threats to the global community. Security agencies often struggle to train machine learning algorithms effectively, leading to poor identification of threats or flawed decision-making related to security (Verhelst et al., 2020). Although AI holds the potential for predicting and preventing terrorist operations, efforts to harness its potential in this area remain limited and uncoordinated (Campedelli et al., 2021). The need to rapidly adapt to shifting threat patterns remains a significant obstacle for security agencies striving to develop and improve their tools.

Individual privacy and national security are two fundamental values that are inherently interconnected yet often in conflict. Therefore, balancing these matters is a challenge. Large-scale data collection can violate privacy, and security agencies must carefully consider the ethical implications of utilizing such technology (Verhelst et al., 2020). Protecting democratic rights and freedoms while remaining practical in fighting terrorism requires international cooperation and the establishment of specialized scientific and practical centers (Bazarkina & Pashentsev, 2019). This challenge must be managed effectively to gain public trust and support comprehensive efforts to strengthen national vigilance against terrorist threats. Terrorist organizations often outpace security agencies in adopting new technologies, leveraging advanced tools, including AI, to plan and execute attacks. AI can be exploited to create sophisticated strategies, spread propaganda, or facilitate secure communications, highlighting the necessity for security agencies to update their strategies and technological resources to remain ahead continuously (Verhelst et al., 2020). For example, terrorist organizations might weaponize drones or use sentiment analysis to identify potential targets based on online human behavior (Bazarkina & Pashentsev, 2019). These advancements increase the complexity of detection and prevention efforts, demanding innovative tools and adaptive approaches.

Data has become one of the most valuable resources across all sectors, including for both terrorist organizations and security agencies. With the overwhelming volume of data available, security agencies must be able to analyze and extract relevant information. This demands significant resources and expertise in data analytics (Verhelst et al., 2020). Terrorist organizations take advantage of this data complexity to recruit skilled individuals, particularly those with strong technical abilities. They use propaganda that appeals to younger audiences, such as programmers and science fiction enthusiasts, to attract recruits. (Bazarkina & Pashentsev, 2019). The challenges encountered by security agencies are precisely the vulnerabilities that terrorist organizations seek to exploit.

Security agencies often face limitations in budget, technological infrastructure, and the availability of skilled human resources for large-scale data analysis. Many agencies, particularly in developing countries, may lack the resources needed to implement advanced technologies and train their staff to use them effectively (Verhelst et al., 2020). With limited resources, security agencies often struggle to respond quickly to emerging threats, mainly when false or manipulative information is spread through technology (Bazarkina & Pashentsev, 2019). Significant investment in developing analytical capabilities can be a major challenge for agencies with limited budgets. AI's involvement in terrorism can lead to long-term consequences, mainly due to its capacity to escalate crises and broaden the scope of attacks. For instance, terrorists might use deepfake technology to create confusion and provoke rapid government responses, potentially leading to hasty military decisions (Bazarkina & Pashentsev, 2019). Additionally, a robot network (botnet) can target multiple systems simultaneously, enhancing both the impact and speed of an attack (Tzezana, 2017). AI-powered attacks have the potential to disrupt financial systems, interfere with communication networks, and even pose a direct threat to national security.

Public involvement is essential in providing crucial information that security agencies might miss. However, engaging the public becomes challenging when many information circulating in the media is sensationalized or misleading (Bazarkina & Pashentsev, 2019). Relying solely on more efficient and robust security forces will not be enough to rehabilitate former jihadis without broader social and cultural changes. National authorities are most effective when they are backed by a variety of Countering Violent Extremism (CVE) strategies (Chalmers, 2017). Countering Violent Extremism (CVE) focuses on preventing and reducing violence driven by extremist ideologies and involves addressing underlying causes such as poverty, injustice, and discrimination. In confronting these challenges, security agencies must adopt more innovative and collaborative approaches to harness technology effectively in the fight against terrorism.

4.2. The Collaborative Impact of Artificial Intelligence and Terrorist Organizations on Terror Operations

The impact of terrorist organizations enhancing their operations with advancements in artificial intelligence (AI) is significantly complex. These organizations can now leverage AI to plan and execute attacks more effectively. For instance, they could use AI-controlled drones to strike physical targets and exploit potential vulnerabilities in their victims (Bazarkina & Pashentsev, 2019). Additionally, machine learning algorithms can help them identify more vulnerable targets and coordinate more precise attacks (Tzezana, 2016). The collaboration between AI and terrorists undoubtedly leads to more destruction than typical conventional terrorist attacks.

The adaptation of terrorist organizations to the vastness of cyberspace brings new methods of carrying out acts of terror. They can leverage technology to gather information, recruit members, plan operations, and spread their ideology. In addition, they can use technology to raise funds and adopt information and communication technology (ICT) for conducting cyberattacks (Broeders et al., 2023). The expansive nature and the lack of boundaries in cyberspace allow these organizations to spread propaganda and recruit individuals with lower risks than in the real world (Jangada Correia, 2022). In many areas with limited law enforcement oversight, terrorist organizations are finding more significant opportunities to expand their operations, adopting more sophisticated and varied tactics to further their agendas.

The collaboration of AI and terrorist organizations dramatically increases the scale and effectiveness of their operations. AI allows these organizations to produce more engaging and personalized content for their intended audiences. They can leverage sentiment analysis and chatbots to identify targets and spread their messages more effectively, increasing the reach and impact of their propaganda (Bazarkina & Pashentsev, 2019) (Prakasa et al., 2021). For example, terrorist organizations might analyze demographic data and user behaviors to pinpoint individuals who are most susceptible to their messages. Additionally, AI can be utilized to optimize the timing and channels for message distribution, further enhancing their effectiveness (Nakissa, 2020). Through data mining techniques, they can analyze extensive datasets to uncover insights that help in crafting more engaging and targeted propaganda campaigns (Correia, 2022). This sophisticated, targeted method of propaganda can pose a more significant challenge for authorities to counter effectively.

Furthermore, the result of advanced technology in terrorist attacks has emerged as a significant threat. AI can be used to identify security weaknesses in systems and execute attacks that impact physical

infrastructure (Tzezana, 2016). Moreover, IoT devices are also potential targets for terrorist operations, as these groups could exploit weaknesses in IoT systems to execute attacks or disrupt critical infrastructure (Yaacoub et al., 2022). In the hands of terrorist organizations, both AI and IoT have turned into dangerous tools; at the same time, if effectively used by law enforcement, these technologies could also become powerful weapons against such groups.

The rise of AI has led to the creation of tools that simplify tasks that once seemed impossible and become more manageable, such as manipulating information and creating deepfakes. Terrorist organizations can exploit deepfake technology to spread false information that incites social unrest or conflicts. For instance, they might issue statements claiming responsibility for attacks, potentially provoking an exaggerated reaction from both the government and the public (Bazarkina & Pashentsev, 2019). AI can be used to avoid detection by law enforcement. Technologies like facial recognition and behavioral analysis can be manipulated to mislead current security measures, making it easier to execute their operations (Tzezana, 2016). Moreover, deepfake technology can propagate misleading narratives that undermine adversaries or governments, leading to confusion and distrust among the public. This strategy can enhance the terrorist message and attract the attention of people who doubt the government's official statements. (Bazarkina & Pashentsev, 2020). In essence, deepfakes serve to distort reality in ways that intensify the threat of terrorism.

AI tools enable terrorists to amplify the complexity and variety of their threats, significantly affecting public safety and escalating the overall risk level. AI allows terrorists to analyze large-scale data and find targets in a short amount of time; terrorists can identify and attack specific individuals or groups efficiently. Such advancements could result in a more excellent atmosphere of insecurity in public. (Bazarkina & Pashentsev, 2019). The use of AI in terrorism can create fear and uneasiness feelings in public. More sophisticated and planned terrorist attacks can increase the psychological impact on the public, which affects social and political stability (Nakissa, 2020). Based on available documents, extremist organizations such as ISIS used cyberterrorism and social media to spread hatred online. The Internet and social media sites serve as a knowledge database that these organizations can use to spread their messages and influence a wider audience (Awan, 2017). The growing threats to public security are a tactic used by terrorist organizations to spread their ideology to wider audiences.

AI's ability to analyze large-scale data, generate compelling content, and adapt swiftly has intensified the complexity of counterterrorism. Overall, terrorist organizations' use of AI has not only increased their ability to carry out attacks but also complicated governments' and security agencies' counterterrorism efforts. The race to anticipate and counter terrorist threats that leverage AI has become a top priority on the global security agenda.

4.3. Potential Scenarios of Cyberattacks by Terrorist Organizations

Analyzing the patterns of terrorist attacks shows that these organizations frequently aim for densely populated areas, especially in urban environments. The rise of technology, particularly AI and IoT, has enhanced urban infrastructures, leading to the development of smart cities. Nevertheless, the advent of smart cities also presents new avenues for threats due to their reliance on online technological advancements. With the help of AI, security agencies can predict possible cyberattack scenarios that could target smart cities. These scenarios are as follows.

a. Cyberattacks Setting before Physical Strikes

These cyberattacks are followed by conventional attacks involving weapons or explosives, leading to considerable disruption and possible loss of life (Tzezana, 2016). The aim is to divert the attention of security forces by disrupting public services and creating chaos within the city.

b. Hackers Disrupting City Operations

Hackers have the potential to cripple or disturb key infrastructure units in a smart city, resulting in political embarrassment, economic damage, and even potential loss of life. Such attacks are highly occurred during major political, sports, or economic events (Tzezana, 2016).

c. Disruption of Smart Grid Network

Due to the heavy dependence of innovative grid systems on computer networks, cyberattacks can disrupt the regular operation of power supply systems. This could result in significant losses in production and daily life, impacting industries such as agriculture and healthcare (Ding et al., 2022). The close interconnection between intelligent grid networks and computer systems makes them particularly vulnerable to cyberattacks by terrorists.

d. Leveraging Vulnerabilities in Smart Grid Networks

Cyberattacks that exploit the vulnerabilities within intelligent grid networks, such as ransomware and malware, can cause significant damage to the power system (Ding et al., 2022). Once infiltrated, malware can rapidly spread, encrypt vital data, and turn off control systems.

e. IoT-Related Attacks on Critical Infrastructure

Power plants, electrical grids, pipelines, and dams are prime targets for IoT-related cyberattacks, which can potentially cause severe disruptions to urban infrastructure (Tzezana, 2017). These scenarios highlight the vulnerabilities of smart cities to cyber threats, which can lead to physical disruptions and have wide-ranging consequences for urban systems.

5. Conclusion

AI technology has been proven to enhance the capabilities of its users significantly, but it can also be misused by terrorist organizations to support or strengthen their operations. AI can be viewed as a double-edged sword; its impact—whether positive or negative—entirely depends on how its users use it. The challenges faced in the future will be increasingly complex due to the use of technology, especially artificial intelligence (AI) by terrorist organizations. These organizations use AI to plan attacks, conduct propaganda, and recruit members in more sophisticated ways, as well as exploit vulnerabilities in critical infrastructure.

The exploitative collaboration between AI and terrorism enhances the effectiveness of terrorist operations, yet it also opens doors for security agencies to anticipate and prevent such actions. Nonetheless, there are ongoing challenges in developing practical algorithms and striking a balance between individual privacy and national security. As terrorist organizations rapidly adopt new technologies, the tasks of detection and prevention are becoming more complicated. Therefore, it is crucial for both the community and government to focus on understanding the combined effects of AI and terrorism, as well as to create comprehensive strategies to tackle the modern security and technological challenges we face.

References

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. Society, 54(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0.

Bazarkina, D. Y., & Pashentsev, E. N. (2019). Artificial intelligence and new threats to international psychological security. Russia in Global Affairs, 17(1), 147–170. https://doi.org/10.31278/1810-6374-2019-17-1-147-170.

Bazarkina, D. Y., & Pashentsev, E. N. (2020). Malicious use of artificial intelligence: New psychological security risks in BRICS countries. Russia in Global Affairs, 18(4), 154–177. https://doi.org/10.31278/1810-6374-2020-18-4-154-177.

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. Studies in Conflict and Terrorism, 46(12), 2426–2453. https://doi.org/10.1080/1057610X.2021.1928887.

Campedelli, G. M., Bartulovic, M., & Carley, K. M. (2021). Learning future terrorist targets through temporal meta-graphs. Scientific Reports, 11(1). https://doi.org/10.1038/s41598-021-87709-7.

Chalmers, I. (2017). Countering Violent Extremism in Indonesia: Bringing Back the Jihadists. Asian Studies Review, 41(3), 331–351. https://doi.org/10.1080/10357823.2017.1323848.

Deslandes-Martineau, D. M., Charland, P., Lapierre, H. G., Arvisais, O., Chamsine, C., Venkatesh, V., & Guidère, M. (2022). The programming curriculum within ISIS. PLoS ONE, 17(4 April). https://doi.org/10.1371/journal.pone.0265721.

Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies, 15(18). https://doi.org/10.3390/en15186799.

Nugrahajati, S. D. and Suparno, B. A. (2024). Program deradikalisasi dalam perspektif komunikasi politik. Jurnal Ilmu Komunikasi, 21(3), 417. https://doi.org/10.31315/jik.v21i3.11440.

Ouedraogo, M., Sanou, D., Kere, I. W. Z., Sankara, S., Thiombiano-Coulibaly, N., Ouedraogo, O., Zoungrana, B., Hama-Ba, F., & Savadogo, A. (2023). Sahel terrorist crisis and development priorities: the case of financial allocations for the control of non-communicable diseases in Burkina Faso. Frontiers in Public Health, 11. https://doi.org/10.3389/fpubh.2023.1253123.

Papyshev, G., & Yarime, M. (2023). The state's role in governing artificial intelligence: development, control, and promotion through national strategies. Policy Design and Practice, 6(1), 79–102. https://doi.org/10.1080/25741292.2022.2162252.

Prakasa, S. U. W., Al-Fatih, S., & Haqqi, A. R. A. (2021). Terrorism Eradication in ASEAN Countries: Human Rights Perspective. Al-Ihkam: Jurnal Hukum Dan Pranata Sosial, 16(2), 327–361. https://doi.org/10.19105/AL-LHKAM.V16I2.5021.

Radil, S. M., & Castan Pinos, J. (2022). Reexamining the Four Waves of Modern Terrorism: A Territorial Interpretation. Studies in Conflict and Terrorism, 45(4), 311–330. https://doi.org/10.1080/1057610X.2019.1657310.

Safira, U. M., Pasaribu, F. H., & Bintang, M. (2017). Isolasi bakteri endofit dari tanaman sirih hijau piper betle l.) dan potensinya sebagai penghasil senyawa antibakteri. Current Biochemistry, 1(1), 51-57. https://doi.org/10.29244/cb.1.1.51-57.

Saidi, F., & Trabelsi, Z. (2022). A hybrid deep learning-based framework for future terrorist activities modeling and prediction. *Egyptian Informatics Journal*, 23(3), 437–446. https://doi.org/10.1016/j.eij.2022.04.001.

Tehrani, P. M., Abdul Manap, N., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law and Security Review, 29(3), 207–215. https://doi.org/10.1016/j.clsr.2013.03.011.

Theowidavitya, B., Muttaqin, M., Miftahudin, M., & Tjahjoleksono, A. (2019). Analisis metabolomik pada interaksi padi dan bakteri. Jurnal Sumberdaya Hayati, 5(1), 18-24. https://doi.org/10.29244/jsdh.5.1.18-24.

Thineza Ardea Pramesti and Mohammad Mirwan (2023). Penurunan tss, cod, dan total nitrogen air lindi dengan constructed wetland menggunakan melati air (echinodorus palaefolius). Jurnal Pengendalian Pencemaran Lingkungan (JPPL), 5(2), 189-195. https://doi.org/10.35970/jppl.v5i2.2010.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. European Journal of Futures Research, 4(1). https://doi.org/10.1007/s40309-016-0107-z.

Tzezana, R. (2017). High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. Foresight, 19(1), 1–14. https://doi.org/10.1108/FS-11-2016-0056

Uddin, M. I., Zada, N., Aziz, F., Saeed, Y., Zeb, A., Ali Shah, S. A., Al-Khasawneh, M. A., & Mahmoud, M. (2020). Prediction of Future Terrorist Activities Using Deep Neural Networks. Complexity, 2020. https://doi.org/10.1155/2020/1373087.

Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma. Science and Engineering Ethics, 26(6), 2975–2984. https://doi.org/10.1007/s11948-020-00254-w.

Wibowo, R. H., Sembiring, S. R., Sipriyadi, S., Darwis, W., Supriyati, R., Hidayah, T., … & Yudha, S. P. (2022). Kemampuan bakteri endofit pelarut fosfat dari tumbuhan akar kuning (arcangelisia flava (l.) merr) asal pulau enggano, provinsi bengkulu. Al-Kauniyah: Jurnal Biologi, 15(2), 171-181. https://doi.org/10.15408/kauniyah.v15i2.17632.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. https://doi.org/10.1007/s10207-021-00545-8.