Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary

Brandon Griffin[1-2], Keitavius Alexander[1-2], Lucas Potter[3], Xavier-Lewis Palmer[2-3]
[1]Old Dominion University, Norfolk, USA
[2]CySecSol, Franklin, USA
[3]BiosView, Oswego, USA

bgrif023@gmail.com
Kalex019@odu.edu
lpott005@odu.edu
xpalm001@odu.edu

Abstract: Biocybersecurity is an evolving discipline that aims to identify the gaps and risks associated with the convergence of Biology (the science of life and living organisms) and cybersecurity (the science, study, and theory of cyberspace and cybernetics) to protect the bioeconomy. The biological industries' increased reliance on digitization, automation, and computing power has resulted in benefits for the scientific community, it has simultaneously multiplied the risk factors associated with industrial espionage and the protection of data both commercial and proprietary. The sensitive and potentially destructive power of this data and its access inherently poses a risk to the national and ontological security of a nation. Ontological security refers to the extent to which an individual or group feels secure in their understanding of the world and their place in it. It is a psychological concept that pertains to the way in which people construct their sense of self and their place in the world, and how this sense of self and place is shaped by their interactions with others and the broader social, cultural, and political context in which they live. Nation-states provide stability and wider social cohesion, but these capacities can be disrupted when the nation state is sufficiently threatened (Bolton, 2021). Leading to an interest in maintaining a national identity; which can have profound effects on the behavior of a nation. Targeted social engineering is aimed at exploiting the changing and damaged mental health of workers in life science enterprises who have not been trained in a sufficient manner to deal with these attacks. Failure to identify the existing vulnerabilities associated with social engineering would expose the bioeconomy to unnecessary risk. Numerous scholars have pointed towards growing risks of nation-state stability being increasingly threatened vs inadequate actions taken to match threats for defense; when reflecting on energy, food, construction materials and more from the multi-trillion US bioeconomy we see that the ground to cover is huge (George 2019, Jordan, 2020, Murch, 2018; Mueller 2021). This paper seeks to discuss some of the existing vulnerabilities associated with social engineering attacks and the effects those attacks would have on the population's ontological security and spark conversations about ways in which ontological security of nation states are modified.

Keywords: Social-Engineering, Bio-economies, Nation-States, Bioveillance, Cyberbiosecurity, Biocybersecurity

1. Introduction

As the digital revolution continues to touch all walks of life the biological industry is no exception. The convergence of digitization, automation, and increased computing power has allowed for the rapid advancement of biological sciences while introducing new forms of risk to each sector of the bioeconomy. The acknowledgement of these threats and their intersections has allowed for the development of Cyberbiosecurity, which has been discussed at length (Murch 2018; Peccoud et al 2018; Murch and DiEuliis, 2019; Duncan et al, 2019; Richardson et al, 2019). Biocentricity of critical resources makes safeguarding the nation take on a different shape and conceptually this requires a more serious approach to STEM and its purveyors within and on behalf of the nation (Murch 2018; George, 2019). A particular threat that has the potential to disrupt both biological professionals and the general population is target social engineering attacks. These are attacks that rely heavily on human interaction and often involve manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations. The potential danger and unwanted consequences of these attacks would be catastrophic to the ontological security of a nation. These three concepts are interconnected and can have a mutually reinforcing effect on one another. Advances in biocybersecurity, for example, may be used to improve social engineering defenses, while social engineering tactics may be used to exploit vulnerabilities in biological systems. Disruptions to ontological security, meanwhile, may affect an individual's or group's ability to effectively defend against cyber threats. By studying these areas together, it is possible to gain a more comprehensive understanding of the complex interplay between them and to develop more effective approaches to addressing the challenges they pose.

2. Core Literature Considered:

Biocybersecurity literature has primarily focused on identifying the gaps associated with the ongoing digitization of the biological science industry. Research into biocybersecurity also seeks to provide recommendations to identify existing threats, and develop frameworks to anticipate, identify, mitigate and deter any hostile nation state or actors from participating in cyber biological attacks. One perceived gap is the lack of discussion surrounding ontological security in the midst of the cyberbio convergence of societies, especially those who are rapidly engaging 4th Industrial Revolution (4IR) technologies. Approaching biocybersecurity, social engineering, and ontological security as a commingled concept can facilitate the development of interdisciplinary approaches and solutions to these challenges. This may involve the collaboration of experts from diverse fields such as computer science, biology, psychology, and sociology, and may lead to the development of more effective and innovative solutions. By bringing together diverse perspectives and expertise, it is possible to gain a more comprehensive understanding of the challenges posed by these issues and to identify more effective approaches to addressing them. These technologies have the potential to more rapidly and specifically change the states of societies at larger scales than prior generation technologies and could use additional discussion. Tables 1 and 2 below respectively show the core literature considered for this work followed by pointing out selected foci in discussion that were helpful for driving this paper.

Table 1: Core Literature Considered

[1] Bolton, D. (2020) "Targeting Ontological Security: Information Warfare in the Modern Age", Political psychology, Vol 42, Issue 1, pp 127-142.	[6]Kavanagh, Jennifer and Michael D. Rich, Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life. Santa Monica, CA: RAND Corporation, 2018.
[2] Ramsey, F., & Seyyedhasani, H. (2021). Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity.	[7] Mueller S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?. Biosafety and health, 3(1), 11–21.
[3] Ferrara, E., Cresci, S. and Luceri, L. (2020). Misinformation, manipulation, and abuse on social media in the era of COVID-19. Journal of Computational Social Science, 3. doi:10.1007/s42001-020-00094-5.	[8] Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. Frontiers in bioengineering and biotechnology, 6, 39.
[4] George A. M. (2019). The National Security Implications of Cyberbiosecurity. Frontiers in bioengineering and biotechnology, 7, 51.	[9] Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape. Frontiers in bioengineering and biotechnology, 7, 99.
[5] Jordan, S. B., Fenn S. L. and Shannon B. B., "Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity," in Computer, vol. 53, no. 10, pp. 59-68, Oct. 2020	[10] G. Rowett, "The strategic need to understand online memes and modern information warfare theory," 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 4437-4442

Table 2: Selected Themes within Focused On

Papers	Selected Foci For Discussion
2, 4, 5, 8,	CyberBiosecurity (Defined)
1, 4, 5, 6, 9	Digitization of Society
5, 7	Social Engineering Risk
1, 2, 3, 4, 6	National & Ontological Security
1,3, 10	Informational Warfare & Social Media

3. National Roles in Ontological Security

The digital revolution has had a unique effect on the ontological security of nation states. Ontological security is defined as "a stable mental state derived from a sense of continuity regarding the events in one's life". Scholars discussing ontological security posit that individuals are not merely concerned with their physical security but also concepts such as their sense of being and perception of stability in their environment (Browning and Joenniemi, 2016). Historically, nation states have played a vital role in addressing this need, providing a stable environment and a national narrative that individuals are embedded within. As civil discourse continues to happen on social media the influence nations once had on the national narrative have effectively been decentralized. This decentralization has created attack vectors for hostile actors to create ontological insecurity through social engineering attacks targeted at the general public and the biological science industry. Throughout the years security professionals have worked to harden the physical systems to prevent unwanted intrusion. Despite being newly acknowledged as a crucial aspect of security engineering, the life sciences sector is not properly equipped to defend against psychological based attacks. Hostile nation states or lone actors are able to gain access to the system through the use of pretext, deception, and contact impersonations. Pretext is one of the quickest ways to bypass an enterprise's defenses, attackers targeting the bioscience fields often masquerade as official tools offering solutions to unique cyberbiosecurity challenges. Attackers lean into the demand for products and services such as research and bioinformatic tools to created complex social engineering campaigns that involve fake websites, and phishing scams that appear to come from official organizations such as HHS (Health and human services), CDC (Center for Disease Control) or WHO (World Health Organization) with the intention to spread harmful software to targeted systems. Attackers may also attempt to impersonate contacts within the target organization to gain access to sensitive data and information. Attackers using specially targeted social engineering messages and techniques seek to exploit these values to cause unwanted harm or intrusion. If the social engineering attack is successful, it would allow the attackers to demoralize, devalue, create distrust, and disenfranchise creators, companies, clients, and more in the biological sciences and biotechnological industries. A map of crucial considerations can be found in Figure 3, illustrating influences via social engineering.

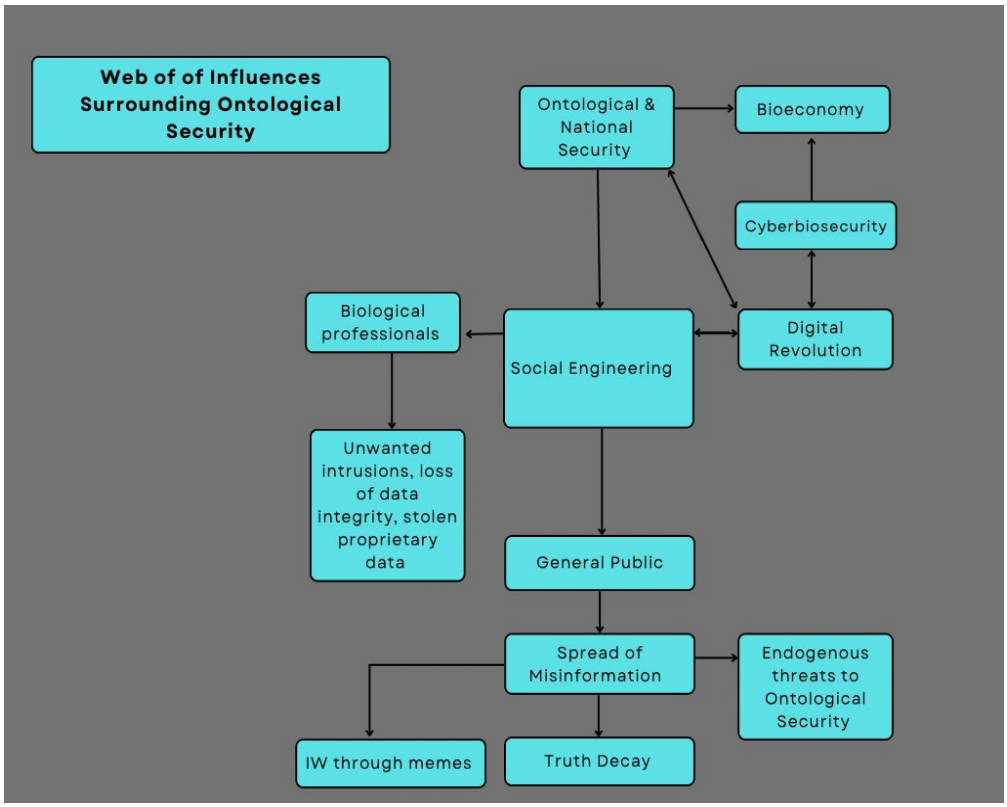

Figure 3: Concept Web of Influences Surrounding Ontological Security

Changes in information systems have allowed for hostile nation states to interfere in the domestic political conversation of their adversaries. The emergence of the internet and social media has amplified the reach of disinformation. Social engineering attacks targeted at the public look to cause ontological insecurity by disseminating truth decay within civil discourse. Truth decay can be defined with a set of four related trends that include: an increase of disagreement and misinterpretation of facts and data, inability to identify fact from opinion, opinion being valued over facts, and a growing in distrust toward respected sources of factual information. Some of the most prominent actors in this truth decay of the past 10 years can be observed within the transition from traditional media to internet and social media (Rich, 2018).

Truth decay helps democratize influence over the national narrative and poses an endogenous threat to ontological security. Endogenous threats occur when the national narrative out of which identity emerges appears disjointed from state behaviors, naturally this causes civil discourse on the topic. By distorting the information environment of the state, truth decay facilitates domestic questions of the congruence between policy and narrative. Cyber espionage can gather information, along with distorted or false information and images, which can be spread among a specific target audience in order to shape their perceptions of national narratives and particular policies or events. That is, leaked information can be distorted and bent towards biased and malicious aims before release to a target public. The possibility of cyber espionage in biological matters has implications for any leaks with the potential to shape national narratives (Bolton 2021). The effects of truth decay can be far reaching and destructive to a nation state, leading to the breakdown of civil discourse, gridlock in the political system, alienation from political and civil institutions and general ontological insecurity (Kavanagh and Rich, 2018). It is important to address truth decay in order to promote a healthy and functioning society.

Industries within the bioeconomy are utilizing and incorporating cyber linked technologies to perform and curate new technologies, perform analysis, log and examine data in real-time, mass produce biological goods, gain in-depth insight like never before, and other essential functions and activities to advance scientific capabilities and knowledge. An advantage of the integration of advanced computation implementation in these industries is the transformation of a more effective, accelerated, and articulated system in which crucial information is obtained and communicated over digital platforms. A key disadvantage is the capacity of attack vectors that cyber threats gaining to these sectors due the the dependence on cyber-linked platforms, devices, and databases. Current technologies of the bioeconomy are already being put to use to provide solutions to key issues such as global warming, agricultural shortages and medical treatments.In modern times, technology such as laptops and smartphones support the development and advancement of agricultural industries. Computing and automation capabilities that smart technology provides has caused major changes in food production (Ramsey and Seyyedhasani, 2021).

Industrial technological tools and biological science work in synchronization to assist processes, productions, analysis, transportation, and other necessary business functions across all sectors. Future technologies of the bioeconomy such as bioengineering could have many applications from cosmetology and to militant biological weaponry. Providing defense capabilities, methods, and resources for the bioeconomy is essential for current and future operation. This extends to considerations to civil engineering in urban planning with pandemics in mind (Potter et al, 2021).

Cyber attackers and adversaries have long since had means to exploit the cyber vulnerabilities in the bioeconomy and we can expect their means to deepen. Current cyber defense and countermeasures should be reassessed to account for ongoing threat evolutions for these systems, the technologies they produce, and the companies and agencies they belong to, and this includes a wider degree of training for personnel and infrastructural upgrade considerations (Duncan et al, 2020; Jordan, 2020; Elgabry et al., 2022). If hostile actors gain access to these core biotechnology intellectual property, a number of consequences could occur; specifically, information of the technology could be leaked to the public out of context or misleadingly with the purpose providing needless or inflated wariness. This in turn harms science communication initiatives and effective public health campaigns.

4. Social Media and Ontological Security

4.1 Role of social media in health promotion and important stakeholders

Social media is a tool in which people communicate on a digital platform sharing pictures, videos, and more digital content. Digital interaction between social media users can occur between different countries and continents. Content can communicate efficiently and quickly. The benefit of this is the creation of a community and ecosystem; professionals and nonprofessionals interact and share knowledge on social media platforms. Medical practitioners utilize social media interfaces to examine, communicate, treat, and triage patients. During critical events such as the COVID-19 pandemic, healthcare misinformation can be spread quickly (Adler et al, 2021; Mueller 2021; Palmer et al, 2021). This cyber access became a necessary component of healthcare in times while people were told to isolate themselves. In some circumstances, social media may be the only means of gaining key information and new detail regarding current healthcare events. Social media provides the platforms for sharing of experiences, education, policies, precautions, and other healthcare content. It is a tool in which healthcare professionals, companies, in industries can perform informational campaigns to better provide knowledge of resources, treatments, struggles, and awareness. New healthcare facilities in poverty stricken communities can be made aware of their proximity and presence and this implication can for non-traditional spaces as well. Overall, social media has given people the ability to communicate vital healthcare information and has proven to be an effective way to promote and increase the spread of translational health communication strategies. It allows users to share, use, and create critical health information and makes advocacy campaigns more efficient by providing a faster means of communication(Stellefson et al, 2020). How it is responsibly supported is vital.

4.2 Pandemic Responses Impacted by Social Media Misinformation

During the COVID-19 pandemic, misinformation was spread all over social media. From the beginning of the pandemic, ignorance of knowledge and details of the coronavirus was exploited, and this was sometimes considered to be through state actor influence and local cyber actors with malicious intent. Researchers at The Center for Countering Digital Hate have concluded that just twelve accounts known as the 'Disinformation Dozen' are responsible for the majority of COVID-19 misinformation across social networking platforms (Imran Ahmed, 2021). This had considerable basis for consideration in terms of asymmetric warfare considerations that malicious parties may invest in (Palmer et al, 2021). Misinformation campaigns against vaccination had a large impact across all social media platforms. This created hesitation, stress, confusion and debate on these vaccinations. Many social media users lacked professional experience, education, and media literacy to filter misinformation and get to necessary information that would be beneficial to their health. The mass of misinformation became such an issue that professionals even faced issues deciphering which content was authentic. Social media platforms had to tag and label which pieces of content were likely to contain misinformation. Some groups of people who lacked social media literacy or likely social usage altogether such as the elderly or technologically illiterate were more likely to be deceived by misinformation or not obtain valid information written by scientific, government, or educational institutions. Cyber threats could use this confusion to exploit non savvy social media users to buy supplements or believe in non verifiable medication such as ivermectin, an anti-parasitic medication rumored on social media to be an effective treatment against the coronavirus (Schellack, 2022). There is no current model to estimate its potential damage to public health (Schillinger, Chittamuru and Ramírez, 2020).Social media platforms attempted to filter out misinformation; however were still unsuccessful due to the large volume of it that still exists and botched means of official curation and messaging. A remaining challenge exists in the ability to support open and well researched dialogue among a public so narrowly trained.

4.3 On Practical Strategies for improving Community Health Literacy

Healthcare industries could create their own links and interfaces that interact with current and emerging social media platforms. Digital campaigns on social media platforms could be curated with the platforms themselves and creatives. Underserved communities, discriminated groups, and unliked social media users should be targeted to encourage engagement with these communities. Inclusivity can provide benefits in emphasis to

cover weak spots in messaging across cultures outside of mainstream habit. Given information to non professional social media users on how to differentiate misinformation from actual research. Social media should provide fundamental education on social media literacy. Relationships between social media platforms and professionals should be developed to create a cyber ecosystem that encourages health literacy. Rather than creating divided sides where content is politicized on social platforms, divided sides of social media users, dialogue discussing matters should be conducted to separate fact from fiction. Patterns, data, and trends of user activity may be analyzed to help healthcare education specialists and other professionals communicate ideologies. Data such as measurements of engagement and experience may help in making future decisions and preventing previous miscalculations and assessing progress of communicating information (Levac and O'Sullivan, 2010; Stellefson et al, 2020). Utilizing social media tools such as analytics can give healthcare professionals additional data to develop relationships and resources for social media platforms and users.

5. The Value of Securing Bioinformatics and databases to the bioeconomy

Emerging and existing technologies boost bioinformatics in examining biological significance and developing technological advances from them. The analytical assets and IP generated from them remain significant targets. A cyber attack from digital adversaries involving social engineering is especially dangerous to the development, reputation, and stability of companies in these industries. A successful attack involving social engineering and informational warfare in which key data on a new technology such as the generation of a cure or treatment through biodetection and bioengineering could result in loss of public trust. In recent times, the COVID-19 MRNA vaccines faced heavy scrutiny on social media due to the purposeful spread of misinformation. Memes, posts, videos, and more digital content were uploaded on many different social media platforms and observed by many. This caused distrust, division, and politicization of this vaccine. The emergence of harmful content on social media platforms that users can encounter in the online ecosystem, specifically regarding the COVID-19 pandemic, represents growing infodemics. This is the uncontrolled spread of information, including a multitude of low-credibility, fake, misleading, and unverified information (Ferrara, Cresci and Luceri, 2020.)

Similar events and circumstances can occur with evolving biotechnologies that utilize digitized bioinformatic systems to operate more efficiently and automated experimentation. Consequences and repercussions will be severe if a cyber threat gained access to a component of one of these systems and obtained sensitive information on the emerging biotechnology. Through means of social engineering and informational warfare, a malicious depiction of the technology could be shared to the world. Misinformation surrounding the technology could be used to sew mistrust in the general public which could have numerous consequences. These consequences include but are not limited to the general public's reluctance to embrace the new technology, the company or agency developing the technology losing financial and social capital, a slowing or ending of the scientific expedition, politicalization of the technology, theft and unauthorized replication of the intellectual property, a knowledgeable threat reverse engineering the development to formulate a weapon, and further cyber attack campaigns from threats to spread more falsehoods about the more technology from the same or similar scientific investigations.

6. Concluding Remarks, Including Limitations

Altogether, not identifying the risk potential of social engineering and informational warfare campaigns targeted at the biological science industry would cause tremendous damage to a nation's national and ontological security. Studying biocybersecurity, social engineering, and ontological security together can provide a more comprehensive understanding of the complex and interconnected nature of cyber threats and the ways in which they can impact individuals and society. By considering these issues in a holistic manner, it may be possible to identify and address potential vulnerabilities more effectively. For example, understanding the psychological mechanisms underlying social engineering tactics may help to develop more effective defenses against them, while understanding the impact of technological change on ontological security may help to mitigate potential negative effects. It is important to also think of how other mediums of relaying information and moods such as through music or video about information may play a role (Omar and DeQuan, 2020: Sice et al, 2020). The information gained from successful social engineering attacks is often used nefariously to question national narratives, inflame domestic policy conversations, and sow distrust among the population. Misinformation

spread through social media is often used by hostile actors to promote truth decay within target nations hoping to increase polarization within domestic politics that are intended to create political paralysis and unravel the bonds of society. There has been a push for biological industry professionals to build relationships and campaigns to help combat the spread of misinformation on the platforms. It is important that the biological industry continues to examine the risk factors associated with attacks that target human psychology. There has also been limited research and information on a systematic approach to educating the general public of the risk associated with social engineering and informational warfare campaigns that happen across social media platforms.

Finally, studying these three areas together can help to ensure that the impact of cyber threats on individuals and society is considered in the development of cybersecurity measures and policies. This can help to ensure that the interests of all stakeholders are considered and that solutions are effective and ethically sound. By considering the social and psychological dimensions of cyber threats, it is possible to develop solutions that are more sensitive to the needs and concerns of individuals and communities, and that take into account the broader societal implications of these issues.

References

Adler, A., Beal, J., Lancaster, M. and Wyschogrod, D., 2021. Cyberbiosecurity and Public Health in the Age of COVID-19. In Emerging Threats of Synthetic Biology and Biotechnology (pp. 103-115). Springer, Dordrecht.

Bolton, D. (2020) "Targeting Ontological Security: Information Warfare in the Modern Age", Political psychology, Vol 42, Issue 1, pp 127-142.

Browning, C. S., & Joenniemi, P. (2017). "Ontological security, self-articulation and the securitization of identity." Cooperation and conflict, 52(1), 31-47.

Carneiro, R., Dunca, S., Ramsey, F., Seyyedhasani, H. and Murch, R. (n.d.). "Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity." [online] Available at: https://caia.cals.vt.edu/content/dam/caia_cals_vt_edu/cyberbiosecurity/2021%20Carneiro%20et%20al%20Cyberattacksinagriculturereprotectingyourfarmandsmallbusinesswithcyberbiosecurity.pdf [Accessed 21 Oct. 2022].

Chen, J., & Wang, Y. (2021). "Social media use for health purposes: systematic review." Journal of medical Internet research, 23(5), e17917.

Duncan, S.E., Zhang, B., Thomason, W., Ellis, M., Meng, N., Stamper, M., Carneiro, R. and Drape, T., 2020. "Securing Data in Life Sciences—A Plant Food (Edamame) Systems Case Study." Frontiers in Sustainability, p.10.

Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E. and Murch, R., 2019. "Cyberbiosecurity: A new perspective on protecting US food and agricultural system." Frontiers in bioengineering and biotechnology, 7, p.63.

Elgabry, M., Nesbeth, D. and Johnson, S. (2022) "The Future of Biotechnology Crime: A parallel Delphi study with non-traditional experts," Futures, 141, p. 102970. Available at: https://doi.org/10.1016/j.futures.2022.102970.

Farsi, D. (2021). "Social media and health care, part I: literature review of social media use by health care providers." Journal of Medical Internet Research, 23(4), e23205.

Ferrara, E., Cresci, S. and Luceri, L. (2020). "Misinformation, manipulation, and abuse on social media in the era of COVID-19." Journal of Computational Social Science, 3. doi:10.1007/s42001-020-00094-5.

Gabarron, E., & Wynn, R. (2016). "Use of social media for sexual health promotion: a scoping review." Global health action, 9(1), 32193.

George A. M. (2019). "The National Security Implications of Cyberbiosecurity". Frontiers in bioengineering and biotechnology, 7, 51.

Jordan, S. B., Fenn S. L. and Shannon B. B., "Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity," in Computer, vol. 53, no. 10, pp. 59-68, Oct. 2020

Rich, M.D., (2018). "Truth decay: An initial exploration of the diminishing role of facts and analysis in American public life." Rand Corporation.

Kavanagh, Jennifer and Michael D. Rich.(2018). "Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life." Santa Monica, CA: RAND Corporation .https://www.rand.org/pubs/research_reports/RR2314.html.

Levac, J. J., & O'Sullivan, T. (2010). "Social media and its use in health promotion." Interdisciplinary journal of health sciences, 1(1), 47-53.

Mwaura, J., Carter, V., & Kubheka, B. Z. (2020). "Social media health promotion in South Africa: Opportunities and challenges." African Journal of Primary Health Care and Family Medicine, 12(1), 1-7.

Mueller S. (2021). "Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?." Biosafety and health, 3(1), 11–21.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy." Frontiers in bioengineering and biotechnology, 6, 39.

Murch, R. and DiEuliis, D., (2019). "Editorial: mapping the cyberbiosecurity enterprise." Front. Bioeng. Biotechnol, 7(235), pp.10-3389

Neiger, B. L., Thackeray, R., Van Wagenen, S. A., Hanson, C. L., West, J. H., Barnes, M. D., & Fagen, M. C. (2012). "Use of social media in health promotion: purposes, key performance indicators, and evaluation metrics." Health promotion practice, 13(2), 159-164.

Omar, B. and Dequan, W. (2020) "Watch, Share or Create: The Influence of Personality Traits and User Motivation on TikTok Mobile Video Usage", *International Journal of Interactive Mobile Technologies (iJIM)*, 14(04), pp. pp. 121–137. doi: 10.3991/ijim.v14i04.12429.

Palmer, X. L., Powell, E., & Potter, L. (2021). Matters of Biocybersecurity with Consideration to Propaganda Outlets and Biological Agents.

Palmer, X., Potter, L.N. and Karahan, S., (2021). "COVID-19 and biocybersecurity's increasing role on defending forward." International Journal of Cyber Warfare and Terrorism (IJCWT), 11(3), pp.15-29.

Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G. and Raman, S., (2018). "Cyberbiosecurity: from naive trust to risk awareness." Trends in biotechnology, 36(1), pp.4-7.

Potter, L., Powell, E., Ayala, O., & Palmer, X. L. (2021). "Urban Planning to Prevent Pandemics: Urban Design Implications of BiocyberSecurity (BCS)." In Intelligent Computing (pp. 1222-1235). Springer, Cham.

Ramanadhan, S., Mendez, S. R., Rao, M., & Viswanath, K. (2013). "Social media use by community-based organizations conducting health promotion: a content analysis." BMC public health, 13(1), 1-10.

Ramsey, F. and Seyyedhasani, H., (2021). "Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity."

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). C"yberbiosecurity: A Call for Cooperation in a New Threat Landscape." Frontiers in bioengineering and biotechnology, 7, 99.

Schillinger, D., Chittamuru, D., & Ramírez, A. S. (2020). "From "Infodemics" to Health Promotion: A Novel Framework for the Role of Social Media in Public Health." *American journal of public health*, *110*(9), 1393–1396. https://doi.org/10.2105/AJPH.2020.3057466.

Schellack, N., Strydom, M., Pepper, M.S., Herd, C.L., Hendricks, C.L., Bronkhorst, E., Meyer, J.C., Padayachee, N., Bangalee, V., Truter, I. and Ellero, A.A., (2022).0" Social Media and COVID-19—Perceptions and Public Deceptions of Ivermectin, Colchicine and Hydroxychloroquine: Lessons for Future Pandemics." Antibiotics, 11(4), p.445.

Sice, P., Elvin, G., Riachy, C., Shang, Y., Ogwu, S. and Zink, C., (2020). "Online screening of X-System music playlists using an Integrative Wellbeing Model informed by the theory of autopoiesis." IEEE Access, 8, pp.182307-182319.

Simpson, V. L., Hass, Z. J., Panchal, J., & McGowan, B. (2022). "Understanding the Development, Evaluation, and Sustainability of Community Health Networks Using Social Network Analysis: A Scoping Review." American Journal of Health Promotion, 36(2), 318-327.

Stellefson, M., Paige, S. R., Chaney, B. H., & Chaney, J. D. (2020). "Evolving role of social media in health promotion: updated responsibilities for health education specialists." International journal of environmental research and public health, 17(4), 1153.

Suarez-Lledo, V., & Alvarez-Galvez, J. (2021). "Prevalence of health misinformation on social media: systematic review." Journal of medical Internet research, 23(1), e17187.

Rowett, G. "The strategic need to understand online memes and modern information warfare theory," 2018