Role of Internet of Things in Biological Warfare

Utkarsha Mahajan

PhD Candidate at the Department of Geopolitics and International Relations, Manipal Academy of Higher Education (MAHE), Manipal, India

Summary

The weaponisation of Information and Communication Technology (ICT) has been a new element in twenty-first century warfare where 'biowarfare' is no exception. Active research has been taking place on the Internet of Things (IoT) domain which finds a wide range of applications in biology. Digitalisation and artificial intelligence have a significant impact on the functioning of microbiology laboratories. The underlying concept of biosecurity, bound by agreements and treaties, fails to incorporate technology as a formal field of study. IoT, a subdomain of ICT, is no exception to be explored as a tool for biowarfare. The impact of the use of biowarfare agents is not visible immediately and can be seen only after an incubation period. Hence, the rapid detection and identification of these agents have become a necessity. Several competitive methods are available to identify the biological warfare agents, where IoT provides an effective solution.

Introduction

With the COVID-19 pandemic, the discussions regarding the changing nature of biological warfare[1] have resurfaced. Biological warfare or biowarfare refers to the intentional use of micro-organisms and toxins to harm humans, livestock, and crops. It has the potential to not only inflict considerable mortality and morbidity but also create a high level of panic, environmental contamination, and extreme pressures on emergency healthcare services. Though the nature of biowarfare has kept changing over the centuries, bioweapons can be identified as systems consisting of two factors i.e., weaponised biowarfare agent and the delivery mechanism.

The history of the use of bioweapons provides evidence of the use of missiles, humans, or air as the mediums for the delivery of the agents. Whereas, over time, more sophisticated and subtle ways of proliferation and dissemination have come into being. Biosensors, for biological warfare agents, serve as simple but reliable analytical tools for the field as well as laboratory assay.[2] Such analytical tools, beneficial for recognising the biological warfare agent and the presence or diagnosis of diseases caused by the agents, are required for adopting adequate countermeasures and to select an effective therapy for the exposed masses. With the growing dependence of individuals' daily lives on the modern interactive digital systems, the vulnerability of the masses to the cyber-attacks has increased multi-fold.

As the Internet of things[3] (IoT) has been revolutionising the modes of interactions between humans and machines, a variety of applications can be seen in several domains including medical R&D, adding to the new ways of creation, delivery and dissemination

of biowarfare agents. The highly networked IoT infrastructure contains a range of integrated circuits, biosensors and bio-identification data. The data collection and its complexity further amplify the need to use advanced technologies to achieve a detailed and structured description of the microbiological data, e.g., the Microbiology Investigation Criteria for Reporting Objectively (MICRO) criteria.[4]

Epidemiological databases can also benefit from structured data. Such databases are highly vulnerable to unauthorised access by adversaries, criminals and terrorist organisations. Most of the medical research facilities and hospitals use state-of-the-art technology for preserving micro-organisms and disease-related information, where IoT applications provide peculiar and effective solutions. Powered by IoT-generated data, Machine learning (ML) has radically changed the mode of handling healthcare-related data that includes information related to clinical microbiological and infectious diseases. The data acquired from IoT devices is processed using ML algorithms at each step of the microbiological diagnostic process i.e., from pre-to post-analytics that helps to deal with the increasing quantities and complexity of data.[5]

With the increasing number of IoT applications in the biological sciences, a large number of subdomains have emerged under IoT such as the Internet of Nano-Things (IoNT), Industrial Internet of Things (IIoT) and Internet of Medical Things (IoMT).[6] The exchange of medical or healthcare-related data between people and medical professionals and medical devices (sensors, monitors, implants etc.) using wireless communication,[7] creates more opportunities for causing biological damage through cyberspace. IoNT can enhance the effectiveness of the provision of combatant defensive kits, which includes smart armour and stealthily active camouflage and medicinal sensors to protect them from chemical and biological agents to serve as the self-healing material.[8]

IoT the Biowarfare: Weaponisation and Agent Detection

The weaponisation of Information and Communication Technology (ICT) has been a new element in the twenty-first century warfare where 'biowarfare' is no exception. The underlying concept of biosecurity which is bound by agreements and treaties, fails to incorporate technology as a formal field of study. IoT, a subdomain of ICT, has not been exempted from being explored as a tool for biowarfare. One of the main challenges that the infectious pathogens and toxins, also referred to as the biological warfare agents, is their dual-use nature. Despite the Biological Weapons Convention (1972) prohibiting the production and stockpiling of the biowarfare agents[9], they can still be legally produced and manipulated for medical or research purposes where therapies, new drugs, vaccines are invented. Though states have signed the convention, the development of pathogens as weapons became the province of clandestine nation-state programs and non-state actor terrorism.[10] The impact of the use of these agents is not visible immediately and can be seen only after an incubation period. Hence, the rapid detection and identification of the biowarfare agents is a need of the hour. A number of competitive methods are available for the identification of these agents. The methods like mass spectrometry along with Chromatography and Polymerase chain reactions[11] (PCR) are some of the widely used techniques for the detection of the agents.

Synthetic biology expands on the possibility of creating new types of bioweapons. DNA synthesis and gene editing can increase the number and severity of the bioterrorists'

threat as mentioned by a U.S. Department of Defense report.[12] The report also identifies three concerns of high priority, including recreating pathogenic viruses like Ebola, SARS or smallpox. The ongoing Covid-19 pandemic has been caused by the agent belonging to the SARS group of viruses.[13] A variant of PCR, called real-time reverse transcription PCR (real-time RT-PCR) is the widely used method for detecting the virus. The reverse transcription process refers to converting RNA to DNA followed by amplification of the DNA for confirming the presence of the virus.[14] As the virologists are desperately seeking solutions for an early vaccine, a cross-disciplinary approach has been actively sought in order to develop adequate monitoring, contact tracing and diagnosing or detecting the virus. Several efforts are being put in developing portable, user-friendly, and cost-effective systems for point-of-care (POC) diagnostics, which could also create an Internet of Things (IoT) for healthcare via a global network.[15]

The 2016 Zika virus outbreak led to the development of a sensitive CRISPR[16]-based biosensor, used to detect a different strain of this virus at low concentration. The application of IoT, big biomedical data, cloud computing, artificial intelligence and signal data obtained from CRISPR-based biosensors or nano-biosensors provide clinical data in the cloud computing system. CRISPR, a powerful technology for gene-editing, has been revolutionising the life sciences and medical research. With the decreasing cost of the technology, CRISPR kits are widely available. A well-connected grid of biosensors integrated with the futuristic CRISPR/Cas's systems to monitor DNA or RNA, connected through GPS, Wi-Fi and Bluetooth using a cloud-based database, will soon be generating a massive amount of data with a range of applications in the telemedicine or e-healthcare systems. Although the data will have restricted access to authorised personnel and institutions. However, these systems are highly vulnerable to attacks by the adversaries, for the misuse of the genetic information. Based on the individual's genotypes and by identifying the weaknesses of the immune system[17], creating more deadly synthetic pathogens make the future biological wars even more destructive.

Another means of IoT weaponisation, in the biowarfare, includes the delivery and dissemination of the biowarfare agents. A variety of spraying devices, weak explosives, pressure vessels can act as parts for the delivery of these biological warfare agents controlled using networked autonomous systems. The remote access to these mechanisms can enable the terrorists to carry out the bio-attack without physically entering the territory or infrastructure.

Internet of Bodies (IoB)[18], an extension of IoT, refers to accessing and controlling the human body via the internet, where autonomous health sensing and actuating systems *aka* closed-loop systems that sense and act towards a biological condition, are used.[19] The IoB systems not only collect a vast amount of biometric data but also can alter the human body's function. The IoB based emerging concepts beyond formal healthcare systems which include Transhumanism, Body hacking and Biohacking are likely to become common practices with their access through smart wearables and smartphones will be available. These activities will not only contribute to the vulnerability to sensitive personal data but also a massive attack that can infringe the body autonomy of the target population.[20]

Mitigating the Biowarfare using IoT

To mitigate the challenge of biowarfare, a well-networked IoT infrastructure is required for monitoring the development and misuse of these biohazardous substances. The preparedness for biowarfare is essential as the origin and identification of Biological weapons are more difficult to recognise than other weapons of mass destruction. Delegated by the Office of Naval Research, a programme was undertaken by the Quantum Leap Innovations, Inc. (QLI) to develop, evaluate, and demonstrate novel technology support to the early detection and rapid response for biological or chemical threats.[21] Other than this, a number of specific technological solutions in Situational Awareness, Course of Action Planning, Command & Control, and Data & Process Integration find applications in the emergency management and force transformation during the biowarfare.

IoT, through an integrated biological warfare framework, can provide an integrated decision support mechanism to address the following challenges of biowarfare:

- Monitoring a biological outbreak
- Identifying the cause of outbreak and source
- Predicting potential exposure
- Planning an effective response and risk reduction strategy
- Notifying the related authorities (such as hospitals, local governments, law enforcement, military, pharmaceutical industries, etc)

The existing state-of-the-art IoT platforms such as the Generative Adversarial Network (GAN)[22], based semi-supervised learning approach for clinical decision support in the health-IoT platform, focus on other health conditions other than pandemic diseases. It improves the classification process and facilitates learning about the illness, and suggests a suitable treatment course. An interoperable Internet of Medical Things (IoMT) platform based on Semantic Web Concepts[23] and the M2M architecture, having doctors as users, have been sought for achieving standardisation.

The Way Ahead

Biomedical data acquired through IoT infrastructure is prone to misuse by adversaries and terrorists for amplifying the infectivity, virulence, and resilience towards vaccines, leading to the severity of the biowarfare leading to a more uncontainable epidemic or pandemic. Biological dual-use specialty represents the character of being used either for peaceful purposes, such as medicine, prevention, protection, or non-peaceful purposes, such as developing and producing biological weapons. Coupling synthetic biology with IoT acquired data can lead to the creation of more lethal biological warfare agents. The development of newer strains of pathogens can develop antibiotic-resistant microorganisms with greater invasiveness and pathogenicity of commensals.[24]

The cross-domain awareness regarding the use of IoT in identifying pathogens and toxins and their delivery and dissemination through networked devices can help the medical research facilities and healthcare systems enhance the security of their control facilities and data storages.

The global health actors such as the World Health Organization, Wellcome Trust, World Bank and the Bill & Melinda Gates Foundation have already developed action plans, protocols, policy documents and research programs.[25] That addresses some

of the current needs and tentatively covers emerging and future priorities, including the biowarfare threats emanating from synthetic biology and the use of cyber means for the launch of attacks. Fine-grained spatial and temporal mapping of physical and biological parameters coupled with the reduced lag between data acquisition and analytics ensures the progress toward real-time analysis for the identification of potential bioweapons. There is an increasing need for statecraft and defence research facilities to prioritise the networked real-time data acquisition and analytics schemes for disaster risk reduction and response for effective preparedness.

The laws regarding genetic and biomedical data sharing via the cloud and access to the IoT and IoB devices need to be more stringent. International debates and deliberations on the biowarfare and prohibition of biological weapons must recognise the dual-use nature of networked systems and hence work towards a cooperative mechanism for the peaceful and constructive use of synthetic biology to prevent the eruption of another more threatening pandemic.

Endnotes:

[1] David P. Clark, Nanette J. Pazdernik, 'Biological Warfare: Infectious Disease and Bioterrorism', *Science Direct*, *Biotechnology (Second Edition)*, pp. 687-719, 2016, available at https://doi.org/10.1016/B978-0-12-385015-7.00022-3, accessed on 5 May 2016.

[2] Miroslav Pohanka, 'Current Trends in the Biosensors for Biological Warfare Agents Assay', *Materials (Basel),* Vol. 12, No. 14, 230318, July 2019, doi:10.3390/ma12142303, available at https://pubmed.ncbi.nlm.nih.gov/31323857/ (doi:10.3390/ma12142303), accessed on 30 May 2021.

[3] Carrie Clickard, *The Internet of Things*. Chicago, IL: Norwood House Press, 2019.

[4] A. Egli, J. Schrenzel, G. Grueb, "Digital microbiology", Clinical Microbiology and Infection, 27 June 2020, available at https://www.clinicalmicrobiologyandinfection.com/article/S1198-743X(20)30367-0/pdf accessed on 2 May 2021

[5] Luz CF, 'Machine learning in infection management using routine electronic health records: tools, techniques, and reporting of future technologies', *Clin Microbiol Infect* 2020, vol. 26, no. 1291e9, available at https://doi.org/10.1016/ j.cmi.2020.02.003.

[6] Abdullahi Umar Ibrahim, Fadi Al-Turjman , Zubaida Sa'id, Mehmet Ozsoz, 'Futuristic CRISPR-based biosensing in the cloud and internet of things era: An Overview', *Springer Nature*, 2020, available at https://doi.org/10.1007/s11042-020-09010-5, accessed on 29 April 2021

[7] Ibid.

[8] Rohan Malhotra, Nano Tech: An Emerging Field In Indian Army's Strategic Defence', Society for the Study of Peace and Conflict, *SSPC Monograph Series No. 1*, July 2019, available at https://sspconline.org/sites/default/files/2019-07/SSPC-Monograph-1-NanoTech-%20RMalhotra_1.pdf accessed on 4 May 2021.

[9] Miroslav Pohanka, 'Current Trends in the Biosensors for Biological Warfare Agents Assay', *Materials (Basel),* Vol. 12, No. 14 230318 July 2019, doi:10.3390/ma12142303, available at https://pubmed.ncbi.nlm.nih.gov/31323857/, accessed on 30 May 2021.

[10] Consensus Study Report,'National Academies of Sciences, Engineering, and Medicine 2018'. *Biodefense in the Age of Synthetic Biology*. Washington, DC, The National Academies Press, 2018, available at https://doi.org/10.17226/24890, accessed on 30 April 2021.

[11] James J Walters, Karen F Fox, A Fox, 'Mass spectrometry and tandem mass spectrometry, alone or after liquid chromatography, for analysis of polymerase chain reaction products in the detection of genomic variation', *Journal of Chromatography* B, Vol. 782, Vol. 1, No.2, 2002, pp. 57-66, ISSN 1570-0232, available at https://doi.org/10.1016/S1570-0232(02)00563-9. (https://www.sciencedirect.com/science/article/pii/S1570023202005639), accessed on 3 May 2021

[12] The National Academies Press, 'Biodefense in the Age of Synthetic Biology', *The National Academies of Sciences, Engineering, Medicine*, 2018, available at https://www.nap.edu/download/24890 accessed on 3 May 2021.

[13] 'Severe Acute Respiratory Syndrome (SARS)', *World Health Organization*, available at https://www.who.int/health-topics/severe-acute-respiratory-syndrome#tab=tab_1, accessed on 29 April 2021.

[14] Nicole Jawerth, 'How is the COVID-19 virus detected using real time RT-PCR?', *IAEA Bulletin*, June 2020, available at https://www.iaea.org/bulletin/infectious-diseases/how-is-the-covid-19-virus-detected-using-real-time-rt-pcr, accessed on 2 May 2021.

[15] Hanliang Zhu, Pavel Podesva, Xiaocheng Liu, Haoqing Zhang, Tomas Teply, Ying Xu, Honglong Chang, Airong Qian, Yingfeng Lei, Yu Li, Andreea Niculescu, Ciprian Iliescu, and Pavel Neuzi, 'IoT PCR for pandemic disease detection and its spread monitoring', *US National Library of Medicine National Institutes of Health*, 11 September 2019, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7125887/ accessed on 3 May 2021

[16] 'CRISPR: A game-changing genetic engineering technique', *Harvard University*, 31 July 2014, available at https://sitn.hms.harvard.edu/flash/2014/crispr-a-game-changing-genetic-engineering-technique/, accessed on 4 May 2021

[17] Stew Magnuson, 'National Security Implications of Gene Editing', *National Defence, NDIA's Business and Technology Magazine,* 26 March 2019, available at https://www.nationaldefensemagazine.org/articles/2019/3/26/editors-notes-national-security-implications-of-gene-editing accessed on 30 April 2021.

[18] Asamanya Mohanty, 'Internet of Bodies (IoB) extends Internet of Things (IoT)- Redefines Future of Bionics and Embedded Systems', Scrabbl, available at https://www.scrabbl.com/internet-of-bodies-iob-extends-internet-of-things-iot—redefines-future-of-bionics-and-embedded-systems, accessed on 3 May 2021

[19] Bhokisham, VanArsdale, Stephens, 'A redox-based electrogenetic CRISPR system to connect with and control biological information networks', *Nature Communication*, Vol. 11, No. 2427, 2020, https://doi.org/10.1038/s41467-020-16249-x, available at https://bioengineeringcommunity.nature.com/posts/internet-of-bodies-iob-using-crispr-to-electrically-connect-with-and-control-the-genome accessed on 30 April 2021.

[20] Mary Lee, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, Bryce Downing, *The Internet of Bodies: Opportunities, Risk and Governance*, 2020, ISBN: 978-1-9774-0522-7, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf, accessed on 1 May 2021

[21] F. Abbott, A. Johnson, S. Prior and Donald Steiner, 'Integrated Biological Warfare Technology Platform (IBWTP). Intelligent Software Supporting Situation Awareness, Response, and Operations', *Semantic Scholar*, 2007, available at https://www.semanticscholar.org/paper/Integrated-Biological-Warfare-Technology-Platform-Abbott-Johnson/6e48c45c09ca657d9213ac241ad4d74c352fabec, accessed on 29 April 2021

[22] Bernard Marr, 'Artificial Intelligence Explained: What Are Generative Adversarial Networks (GANs)?', *Forbes*, 12 June 2019, available at https://www.forbes.com/sites/bernardmarr/2019/06/12/artificial-intelligence-explained-what-are-generative-adversarial-networks-gans/?sh=3b886f917e00 , accessed on 4 May 2021.

[23] Karin Koogan, Breitman Marco, Antonio Casanova, Walter Truszkowski, *Semantic Web: Concepts, Technologies and Applications*, Part of the NASA Monographs in Systems and Software Engineering book series (NASA), 2007, ISBN: 978-1-84628-581-3, available at https://doi.org/10.1007/978-1-84628-710-7

[24] Ramesh C, Gupta D, Thavaselvam, Swaran S. Flora, 'Chapter 30 - Chemical and biological warfare agents', Biomarkers in Toxicology, Academic Press, 2014, pp. 521-538, ISBN 9780124046306, available at https://doi.org/10.1016/B978-0-12-404630-6.00030-0 accessed on 3 May 2021

[25] David Thaler, Michael Head, Andrew Horsley, 'Precision public health to inhibit the contagion of disease and move toward a future in which microbes spread health', *BMC Infectious Diseases*, 06 February 2019, available at https://doi.org/10.1186/s12879-019-3715-y accessed on 2 May 2021