# The Convergence of Biological and Cyber Warfare

Krutika Patil

*Krutika Patil is Research Assistant, Cybersecurity Project, MP-IDSA*

**Summary**

Concerns about cyber threats have grown as a result of the COVID-19 pandemic-ravaged global order. Our biological and digital systems have been severely damaged by the proliferation of different virus varieties. It is crucial to envisage convergence points for biological and cyber warfare for a post-pandemic world order since the COVID-19 pandemic resembles a form of biological warfare combined with persistent cyberattacks. There are two points where biological and cyberwarfare converge. Firstly, integrating cyber and biological weapons might have disastrous results resembling a new form of warfare. Second, the development of international norms for cyberwarfare might learn a lot from the enormously successful development of norms for biological weapons, which are prohibited by international law, given the similarity in their threat characteristics.

## Introduction

In the 1990s, cyber warfare was merely a theoretical concept. The situation is visibly different in the 2020s as showcased by the Russia-Ukraine conflict where both sides have employed offensive cyber capabilities.[1] The pandemic-ridden global order has only exacerbated cyber threats-related concerns. The escalation of virus variants has wreaked havoc in our biological and digital systems. Dangers in post-pandemic cyber space pertain to surge in cyberattacks on critical infrastructure, spyware threat, pandemic espionage, disinformation campaigns, rising cybercrimes, and ransomware proliferation due to an inescapable compulsion to digitise.[2]

Therefore, since the COVID-19 pandemic resembles a form of biological warfare coupled with relentless cyberattacks, it is imperative to conceptualise convergence points for biological and cyber warfare for a post-pandemic world order. The intersection of biological and cyber warfare appears at two points. Firstly, the consequences of combining cyber and biological weapons could be catastrophic. While biological warfare has traditionally been viewed as a threat requiring the presence of a specific biological agent, the rise of cyber warfare campaigns has led to the emergence of a fifth phase of bio warfare with a "cyber-bio" framing.[3] Secondly, due to their similarities in threat characteristics, the international norm setting for cyber warfare could gain tremendously from the hugely successful international norm building for biological weapons that are prohibited under international laws. The analysis of these convergence points is essential for tackling new biological and cyber warfare threats and to find possibilities of international restrictive

norm-setting strategies for a post-pandemic offensive cyber capability of countries.

## Combined use of Biological and Cyber Weapons

Biological warfare, or the use of pathogenic bacteria and viruses, or toxic biological substances to kill, sicken, or confuse an enemy, has been practised for thousands of years.[4] Biological warfare has traditionally been viewed as a threat that emerged from four distinct eras: pre-germ theory, applied microbiology, industrial microbiology, and molecular biology and biotechnology.[5] Comparably, in cyber warfare, computer networks are used to disrupt, deny, degrade, or destroy information on enemy computers and networks, or even the computers and networks themselves.[6] When cyber and biological weapons are used together, the results can be disastrous. A country that possesses both weapons may be tempted to use both at the same time in order to multiply the damage. For instance, a nation may launch a cyberattack to gain access to sensitive data on the enemy's bioweapon capabilities, including protective equipment and vaccination stocks.[7] Therefore, by weaponizing or virtually amplifying natural epidemics, bio-warfare in the fifth era seeks to weaken socio-political systems rather than directly causing mortality and morbidity in populations through the use of dangerous biological agents.[8] The combinational use of cyber and biological weapons through IoMT (Internet of Medical Things) cyberattacks, critical medical infrastructure breaches, disinformation and misinformation campaigns, and pandemic espionage, can intensify the deleterious effects of biological warfare.

### *Internet of Medical Things (IoMT) Cyberattacks*

To enhance medical treatment and research, the pharmaceutical and healthcare sectors are progressively integrating new technology into their systems. The IoMT refers to devices that are linked to healthcare IT systems via network connections, and is rapidly expanding, with hospitals, patients, and medical professionals using connected devices for various medical functions.[9] A part of the IoMT are the Implantable Medical Devices (IMDs), that include implantable cardiac defibrillators, cochlear implants, insulin pumps, pacemakers, and neuro-stimulators. There are increasing concerns of the security integrity of these devices as they are susceptible to hacking.[10] In June 2020, researchers identified a group of 19 vulnerabilities in a TCP/IP software library, called Ripple20. These flaws affect a number of medical devices and could be exploited for a range of nefarious purposes, such as reducing or obstructing device functioning. Devices used to deliver low-voltage electrical stimulation to the brain to manage chronic pain are vulnerable to attack and can be hacked to change voltage settings.[11] From the standpoint of cyberspace security, this is undoubtedly a brand-new form of biological warfare.

### *Critical Medical Infrastructure Breaches*

A biological attack combined with a cyberattack can shut down hospital information technology systems that may result in widespread casualties. Threat actors can execute a biological attack while also interfering with hospital operations using malware. In fact, health-related cyber networks are not subject to the same strict cybersecurity regulations as other sectors, such as energy or financial services, despite demonstrable attacks showing that the healthcare industry is a key target among critical national infrastructure sectors. For example, the 2017 WannaCry ransomware attack paralyzed the National Health Service

(NHS) of the United Kingdom, disrupting one-third of hospital trusts, damaging 1 per cent of NHS computers, costing £92 million, and cancelling 19,000 patient appointments. These breaches may also be lethal. In the midst of the COVID-19 pandemic in October 2020, US government agencies issued a warning about an upsurge in ransomware attacks against hospitals by threat actors with ties to Russia employing Trickbot and Ryuk malware to destroy critical US healthcare infrastructure.[12]

*Disinformation and Misinformation Campaigns*

Disinformation campaigns that target public health institutions and policies have increased tremendously, giving rise to widespread anti-vaccination movements and undermining domestic and global responses to outbreaks and pandemics. The rise of measles cases following disinformation campaigns related to the US 2016 presidential elections, the rise of disinformation during the COVID-19 pandemic, and the impact of misinformation on public health interventions during the Ebola outbreaks in 2014-2016 in West Africa and those in 2019-2020 in the Democratic Republic of the Congo are a few examples to explain this phenomenon. High levels of scientific reporting and official advice are juxtaposed with large-scale media reporting, conflicting statistical interpretations, rumours, and hypotheses using disinformation and misinformation. These active disinformation tactics, combined with misinformation disseminated via social media, are likely to exacerbate the outbreak by increasing public distrust of official reporting and rejection of scientific data.[13] The impact of disinformation on pandemics can be compared to a bio-cyber phase, a new stage in biological warfare in which an outbreak is essentially weaponized to have effects similar to biological warfare but without having to deploy an actual virus, avoiding international repercussions.[14]

*Pandemic Cyber Espionage*

Cyberattacks aimed at stealing COVID-19-related information have become widespread. North Korean hackers, for example, attempted to breach the systems of Pfizer, a pharmaceutical company that manufactures COVID-19 vaccines. Meanwhile, some Portuguese-speaking cyber criminals gained access to the computers of Oxford University researchers involved in COVID-19 vaccine research. Russian and Chinese intelligence agencies have been accused of attempting to steal data on COVID-19 medicines and vaccines from the European Medicines Agency in 2020. Interestingly, the Lithuanian government claimed that Russian hackers were using the country's IT infrastructure to conduct cyber espionage against organisations dealing with the COVID-19 vaccine.[15] Therefore, the cyber espionage related to the pandemic facilitates and sets the groundwork for biological warfare.

## Similarities between Cyber and Biological Warfare

Cyber and biological weapons have been adequately compared to nuclear weapons. For instance, according to Joseph S. Nye Jr., despite significant distinctions between cyberattacks and nuclear weapons, governments and private players can apply nuclear lessons to understand and handle cyberspace[16] and bioweapons being referred as the 'poor man's atomic bomb', as a deterrence strategy for nations that cannot afford to develop nuclear weapons.[17] However, while it may seem that dangers

posed by biological and cyber weapons have nothing in common, they actually have a number of similarities that have a significant impact on global security. These weapons have been described as 'non-explosive' weapons in the category of 'non-obvious' warfare, because both the identification of the opposing force and the nature of war are entirely unknown.[18] Gregory Koblentz and Brian Mazanec have classified the similarities between cyber and biological warfare into seven commonalities: 1) the difficulty of attribution; 2) attractiveness as an asymmetric weapon to weaker powers and non-state actors; 3) unclear deterrence value; 4) dual-use nature of affiliated technologies; 5) force multiplier capabilities in the battlefield; 6) penchant for significant collateral damage; and 7) adoption of clandestine programmes to develop these weapons.[19]

The **challenge of attribution** with these weapons is due to their ability to be deployed covertly from unidentifiable or proxy locations and the defender's lack of access to tools to reliably track down the perpetrator of the attack. These weapons are ideal for carrying out clandestine operations and often the victims aren't even aware that an attack has taken place due to the weapon's delayed effects. Just like in biological warfare, it is difficult to differentiate between natural and man-made outbreaks, in cyber warfare, it is a laborious task to identify if a breach was intentional or a technical glitch. It is technically difficult to link a pathogen or computer virus to a specific laboratory or geographic region. For example, The 2001 anthrax letter attacks, in which dried spores of the bacterium Bacillus anthracis, which causes anthrax, killed five people and cost the United States $6 billion, illustrated the difficulty of identifying the source of a biological attack.[20] Further, even after two years since the COVID-19 pandemic, that killed 5 million people and affected 300 million people globally, the exact location and data on how the initial outbreak took place in China, still remains a mystery.[21] The question of attribution is even more contentious in cyberspace. This invisibility cloak due to lack of a mechanism for attribution helps perpetrators to wreak havoc without any accountability.

Historically, the discussions on taming these weapons have been challenging because of their **dual-use applications** and their much-desired ability to act as force multipliers in the battlefield. Commercial, off-the-shelf technology can be used to develop both biological and cyber weapons, which have numerous peaceful and lethal applications along with civil and military ones. Further, due to its multi-use potential, anonymity, widespread effects and relatively low costs, these asymmetric weapons are extremely **attractive for the non-state actors and weaker powers.** For biological warfare, dangerous organisms or toxins can be obtained from natural sources or under the guise of a peaceful application, such as academic research. Similarly, in cyber warfare, the regulation on cyber weapons due to the ubiquity in dual-use application is even more challenging. Botulinum toxin, for example, is one of the most lethal substances on the planet and can be a highly effective biological warfare agent. It is, however, widely used in an extremely diluted form to treat muscle spasms and wrinkles via cosmetic botox treatments.[22]

The capacity to employ these asymmetric weapons as a **force multiplier in conventional military operations** is a significant similarity between biological and cyber warfare. Cyber weapons are particularly suited for employment at the operational, or theatre, level of warfare to cause operational paralysis, decreasing the

enemy's capacity to deploy and coordinate forces in the theatre, as seen in the most recent conflict between Russia and Ukraine.[23] Similarly, the prolonged period of illness caused by some biological agents, such as Brucella spp., may counterbalance the delayed time of onset. The advantage of incapacitating agents is that they would force the defence to deal with many wounded soldiers, who normally use up more resources than dead soldiers do.[24] Further, another common feature is the **unpredictability** associated with the use of biological and cyber weapons, as well as the **potential for collateral damage** as a lack of operational experience with these weapons makes understanding and optimising their effectiveness difficult.

In addition, the capacity to act as a **strategic deterrent is significantly reduced** due to the unpredictable consequences of biological and cyber weapons, the accessibility of defences against them, and the necessity of secrecy and surprise for these weapons to be effective. Finally, another feature that is shared by biological and cyber weapons is the **use of covert programmes** to develop them. Both of these weapons are sensitive enough and their development is rarely acknowledged. The concealed nature with which States develop cyber and biological warfare programmes makes it more difficult to detect and understand them. For instance, the Soviet Union possessed the largest biological weapons programme in history and for decades its magnitude, scope, and sophistication was kept a secret.[25] Similarly, the effects of the Edward Snowden episode, that leaked the extent of the United States government's surveillance programme, is only indicative of how in order for the usage of these weapons to be successful, their development needs to be secretive.[26]

## Mutual Norm Setting Lessons for Biological and Cyber Weapons

While biological and cyber warfare share various similar threat characteristics, there are also significant differences. The main dissimilarity being the direct impact of biological weapons on human beings, which is indirect in cyber weapons. Therefore, for cyber weapons to have direct physical implications, they need to anchor a vector, which is not the case with biological warfare. Moreover, there is a long history associated with poisons, which provides a context for thinking about biological weapons that cyber weapons lack due to their relatively new origins that operate in a new and man-made domain, and lack a similar historical, normative framework.[27] However, the development of biological weapons is prohibited by international treaties and nations run the risk of invoking retaliatory measures like economic sanctions. Therefore, due to a number of similarities, as well as the knowledge and rich history of dealing with biological weapons, tactics to counter cyber weapons could advance faster, by learning from the experience of biological warfare, such as the potential for developing restrictive international norms.

### *Norm Setting for Biological Weapons*

Despite being categorised as weapons of mass destruction after nuclear weapons, biological weapons are much older than nuclear weapons and have been in use since ancient times. The Biological Weapons Convention (BWC) now prohibits the development, production, and stockpiling of biological weapons. This event, which prompted the creation of numerous strategies for addressing the threat presented by biological weapons, including international treaties, deterrent threats, export controls, and physical and medicinal countermeasures, has an important historical context. For

example, Germany launched the first State-sponsored biological warfare programme during the First World War in an attempt to weaken the Allied war effort. Both the Allies and the Axis powers developed biological weapons during the Second World War, and Japan employed them against Chinese soldiers and civilians. Furthermore, several countries, including the United States, the Soviet Union, the United Kingdom, France, Iraq, and South Africa, continued to pursue offensive biological warfare programmes during the Cold War.[28]

Numerous countries took unilateral steps to eliminate their stockpile of biological weapons during the 1960s and 1970s. In 1969, the United States stopped using biological weapons, destroyed its stockpile, and ended its 27 years old offensive biological weapons programme.[29] Britain and France too abandoned their biological weapons programmes after becoming nuclear weapons states. Following unilateral disarmament efforts by various States, the BWC was negotiated and opened for signature in 1972, becoming the first treaty to prohibit an entire class of weapons, which came into effect in 1975. Despite the absence of verification procedures in the treaty, the BWC's main objective was to stigmatise and delegitimise biological weapons by enforcing international norms against their creation, ownership, and use. This was demonstrated by the Soviet Union's secret expansion of its biological weapons programme for over a decade even after it had signed the BWC and publicly renounced bioweapons.[30] In addition, because verification procedures for the BWC could not be agreed upon when the treaty was signed due to increased hostility between the United States and the Soviet Union during the Cold War, the treaty's significance is purely declarative.

Nonetheless, unlike the Non-Proliferation treaty, the BWC was an impartial treaty with the same binding rules for all stakeholders. The BWC currently has 183 states-parties, including Palestine, and four signatories (Egypt, Haiti, Somalia, and Syria). Ten states have neither signed nor ratified the BWC.[31] Since its initiation, the BWC has been enhanced by the addition of measures that foster confidence, such as notification of plague outbreaks, notification of bioterrorism incidents, and the development of security labs. The success of BWC and unilateral abandonments of these weapons suggest that these weapons were not considered to be absolutely useful. This may also be seen in the fact that terrorists have not used biological weapons since they are less effective and efficient than easily accessible conventional methods.[32] However, norms setting may still be one of the most effective methods for mitigating cyber danger, despite the failure of norms and international agreements to restrain some biological weapons programmes.

*Norm Setting for Cyber Weapons*

When it comes to norm setting for restrictive use of cyber weapons, States particularly struggle with agreeing on common objectives. The disparity emerges because Russia and China emphasise on the value of sovereign control while other democracies support a more open internet protocol. International norms setting for cyber weapons began in 1998 when Russia proposed a United Nations (UN) treaty to ban 'electronics and information weapons'. This proposal was supported by China and other Shanghai Cooperation Organisation members (India was not a member when SCO was established in 2001). The US, however, blocked this effort due to its strategic superiority in these technologies. Nonetheless, in 2004, the US and 13 other States agreed to the Russian proposal after which the UN Secretary General appointed a group of governmental experts (UNGGE)

to discuss the issue of cyber threats. Since then, five GGEs met in response to the United Nations First Committee Resolution on 'Developments in the Field of Information and Telecommunications in the Context of International Security.' The lethargy in cyber-related norm setting has been due to the difficulty in accepting common nomenclature; for example, the Russians prefer the term 'information warfare', whereas the US prefers 'cyber operations'. However, the GGE issued reports in 2010, 2013, and 2015 that helped to shape the cybersecurity negotiating agenda significantly. However, the 2017 GGE meeting was a failure and the members could not agree on a common agenda.[33] The UN General Assembly also established an Open-Ended Working Group (OEWG) in 2019 as a parallel working group with GGE on ICTs in the context of international security.[34] Therefore, clearly in comparison to norms setting for biological weapons, work on cyber weapons has a long way to go for encouraging restrictions and bans.

The vast expertise with biological warfare stands in stark contrast to the very little experience with the increasing danger of cyber warfare. The most important lesson from the BWC for a cyber-weapon convention is whether or not effective verification is possible, meaning if stakeholders can pinpoint on necessary conditions to sign and even ratify an arms control treaty. As evident in the BWC, even though bioweapons are banned, the mechanism to verify if States have or are developing bioweapons is absent. Therefore, if inherent verification barriers are taken into account, cyber weapons appear to be one of the worst candidates for an arms control treaty. Cyber weapons pose far more difficult verification challenges than biological weapons due to their attribution challenges, dual-use nature, and development in covert programmes. Further, the success of ban on bioweapons has been due to limited tactical and strategic utility of these weapons.[35] It is unclear on how States can be convinced of tactical and strategic limitation of cyber weapons in the long run, as they are now effectively employed by various militaries as force-multipliers. This can perhaps be possible through the stigmatisation of cyber warfare and its weapons similar to the strategy employed for norm setting for biological weapons. In addition, to successfully implement a dissuasion strategy against cyber weapons, nations and societies must agree that information technology advancements should only be used for peaceful purposes and that using cyber weapons to attack civilian targets and vital infrastructure is unacceptable. The Quad's approach to strengthen cyber resilience through its various initiatives is one example of norm setting strategy that must be expanded beyond the Indo-Pacific.[36]

## Endnotes:


1 Joshua Rovner, "Sabotage and War in Cyberspace", *War on the Rocks*, 19 July 2022.

2" Major Events and Trends in Cybersecurity in 2021", Cybersecurity Centre of Excellence, Manohar Parrikar Institute for Defence Studies and Analyses, 2022.

3 Rose Bernard et al., "Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare", *Infodemics and Health Security*, 18 Febuary 2021.

4 Gregory Koblentz and Brian Mazanec, "Viral Warfare: The Security Implications of Cyber and Biological Weapons", *Comparative Strategy*, 8 November 2013.

5 Rose Bernard et al., no. 3.

6 Gregory Koblentz and Brian Mazanec, no. 4.

7 Ghita Mezzour, "Assessing the Global Cyber and Biological Threat", Carnegie Mellon University, 1 April 2015.

8 Rose Bernard et al., no. 3.

[9] Rose Bernard et al., "Cybersecurity and the unexplored threat to global health: a call for global norms", Global Security: Health, Science and Policy, 29 December 2020.

[10] Jay Liebowitz and Robert Schaller, "Biological Warfare Tampering With Implantable Medical Devices", *IT Professionals*, 21 September 2015.

[11] Rose Bernard et al., no. 9.

[12] Ibid.

[13] Rose Bernard et al., no. 3.

[14] Rose Bernard et al., no. 9.

[15] "Major Events and Trends in Cybersecurity in 2021", no. 2.

[16] Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, January 2011.

[17] Tyler Headley, "Introducing "the Poor Man's Atomic Bomb": Biological Weapons", *National Interest*, 2 December 2018.

[18] Gregory Koblentz and Brian Mazanec, no. 4.

[19] Ibid.

[20] Ajay Kumar Goel, "Anthrax: A disease of biowarfare and public health importance", World Journal Clinical Cases, 16 January 2015.

[21] William Yang, "COVID two years on: World still awaits answers about virus origin", *Deutsche Welle*, 11 January 2022.

[22] Ram Kumar Dhaked et al., "Botulinum toxin: Bioweapon & magic drug", Indian Journal of Medical Research, November 2010.

[23] "Ukraine at D+104: Cybercrime as a force multiplier", The CyberWire, 8 June 2022.

[24] Gregory Koblentz and Brian Mazanec, no. 4.

[25] Raymond A. Zilinskas, "The Soviet Biological Weapons Program and Its Legacy in Today's Russia", National Defense University Press, 18 July 2016.

[26] "Edward Snowden: Leaks that exposed US spy programme", BBC News, 17 January 2014.

[27] Gregory Koblentz and Brian Mazanec, no. 4.

[28] Cameron S. Brown and David Friedman, "A Cyber Warfare Convention? Lessons from the Conventions on Chemical and Biological Weapons", The Institute for National Security Studies, 2014.

[29] Gregory Koblentz and Brian Mazanec, no. 4.

[30] Ibid.

[31] "Biological Weapons Convention Signatories and States-Parties", Arms Control Association, March 2022.

[32] Cameron S. Brown and David Friedman, no. 28.

[33] Joseph S. Nye, "Normative Restraints on Cyber Conflict", Belfer Center for Science and International Affairs, August 2018.

[34] "Open-ended Working Group", United Nations Office for Disarmament Affairs.

[35] Cameron S. Brown and David Friedman, no. 28.

[36] Krutika Patil, "Quad and Cybersecurity", Manohar Parrikar Institute for Defence Studies and Analyses, 22 June 2022.