Future Bioterror and Biowarfare Threats for NATO's Armed Forces until 2030

Dominik Juling

Abstract: The article argues that advances in biotechnology and other transformations of the threat environment will increase the risk for North Atlantic Treaty Organization (NATO) forces of being confronted with a biological, particularly a genetically modified, weapon by 2030.
Keywords: bioweapon; biowarfare; bioterrorism; chemical, biological, radiological, and nuclear; CBRN, future warfare

Introduction

At the beginning of the COVID-19 (coronavirus disease) pandemic, caused by the virus SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2), the dangers posed by biological attacks or the strategic effects of pandemics were discussed in national security debates. Now, one catastrophe follows the next, and the Russian war of aggression dominates the security agenda. In the foreseeable future, however, we will not be able to erase new, natural biological threats from the agenda. For example, the 2022 monkeypox outbreak, with a first outbreak cluster in the United Kingdom, reminds us that smaller outbreaks of transmissible diseases are a constant companion of humanity. Nevertheless, the security dimension of pathogens has fundamentally changed in the twenty-first century. It will change even more in the future.

This article explores the next generation of warfare in terms of biological threats by the year 2030. Because of few precedents in the area of biological warfare or biological terror and the partial look into the future, the article, and especially its target audience and substantive focus, is broad. Because biological

Dominik Juling studies conflict studies at the London School of Economics and Political Science and environmental science at Yale University. Previously, he graduated from the Technical University of Munich in political science with a focus on technology. He has work experience with the German Armed Forces, NATO, and the George C. Marshall European Center for Security Studies. His academic interests are diverse but mainly focus on the interaction of climate change and conflict.

Journal of Advanced Military Studies vol. 14, no. 1
Spring 2023
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20231401005

threats often involve difficult-to-control spread of germs, North Atlantic Treaty Organization (NATO) forces were chosen as the major threatened group for this article, rather than focusing on the U.S. Marine Corps alone. Consistent with the U.S. Marine Corps' *Force Design 2030* and the *NATO 2030* initiative, the time horizon of 2030 was chosen. The former is a comprehensive modernization and restructuring program for the U.S. Marine Corps within the 2030 time horizon. Key points of the program include modernizing equipment, improving cooperation with the U.S. Navy, adapting tactics and strategy to modern weapons, threats and surveillance technology, and better internal talent management. While the *Force Design 2030* report talks a lot about emerging military technologies and hostile area denial, it does not talk about the possibility of biological methods of area denial and their countermeasures. This article is intended to draw attention to potential threats that must also be considered in the restructuring of the U.S. Marine Corps.[1]

Within the framework of the *NATO 2030* initiative, an innovation and reorientation plan comprising nine proposals, it states that NATO also wants to defend its technological lead in the field of biotechnology. In addition, NATO's new Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy, which has been in place since 2022, provides a comprehensive overview of NATO's policy on biological threats, but it often remains comparatively vague. This article will help to provide examples and further information on threats.[2]

The threats studied may stem from state actors, nonstate actors, unknown origins, or accidents. Consequently, the research question is: "What are possible future bioterror and biowarfare threats for NATO's Armed Forces by 2030?" While past and current events and examples are used throughout the article, the goal is to identify and broadly assess potential future threats. The hypothesis for the article thus assumes that advances in biotechnology and other transformations of the threat environment will increase the risk for NATO forces of being confronted with a biological, particularly a genetically modified, weapon by 2030. The article will show how and why the author comes to this conclusion. In doing so, the article will attempt to demonstrate that future biological threats by 2030 pose a serious but underestimated threat to NATO.

To provide an entry point and broad overview of the topic, the article provides a short history of biowarfare and bioterrorism and discusses the future biological threat environment, influential megatrends, emerging and disruptive technologies, possible biological threats by 2030, current and future means of delivery, and possible actors. It is argued that the threat from deliberately deployed biological agents will increase and change in nature by 2030. Unlike, for example, chemical weapons, biological weapons have not been tactically or strategically usable against humans because of their potentially uncontrolled spread, even to unprotected friendly forces, coupled with their highly complex production and stabilization outside of laboratory conditions. However, advances in biotechnology in modifying existing pathogens and creating entirely new ones now make it possible to circumvent these previous barriers and

produce limited biological weapons for the first time. At the same time, it has already become cheaper, easier, and safer to produce dangerous agents, even more so by 2030. New technologies are also helping to deliver biological agents more effectively. In dual-use terms, by 2030 numerous civilian biotechnological successes will create a vast array of possibly ill-intentioned weapons that will provide NATO's hostile actors with a wide range of methods.

History of Events and Developments Involving Potential Biological Weapons until 2022

As early as 1932, Japan engaged in a massive biological weapons program that resulted in the deaths of at least 10,000 prisoners of war by 1945. It is estimated that more than 200,000 additional civilians and soldiers were killed by Japanese biological weapons during military field operations. Various pathogens and means of delivery were systematically studied. After the end of the Second World War, further nonlethal experiments with biological weapons were conducted by the United States.[3] Particularly noteworthy are the results of a series of ethically highly controversial experiments on unknowing civilians in America. At that time, about 800,000 people in San Francisco were infected with a harmless bacterium. A ship was used to disperse the organisms in the air, but a dispatch with airplanes is also known. In secret tests in the New York City subway, there were even more estimated infections with the harmless bacteria noted. Light bulbs filled with microbes were thrown onto the tracks to distribute the bacteria. At least 239 known tests were conducted between 1949 and 1969, demonstrating the potentially massive spread of deliberately released bacteria.[4] The Soviet Union had a similarly comprehensive biological weapons program. In 1979, four years after the Biological Weapons Convention came into force, there was a very serious accident involving anthrax spores in a laboratory in what is known today as Yekaterinburg, Russia. Due to a missing filter, the area around the laboratory was contaminated and at least 66 people died.[5] Based on testimony from high-level former employees of the Soviet Biopreparat Research Agency, it can be inferred that the Soviet Union worked intensively to develop, mass produce, and test delivery methods of highly lethal biological weapons. Strains were repeatedly modified and improved. The goal was to create weapons that avoided precautionary measures or aftertreatment and were effective quickly and lethally.[6]

The first significant attack in modern history using bioweapons and defined as terroristic occurred in 1984, when followers of cult leader Bhagwan Shree Rajneesh infected 751 citizens of The Dalles, Oregon, with salmonella. Forty-five people were hospitalized. The precipitator was the sect's intention to gain seats in the local county circuit court.[7] In 1990, another cult began more comprehensive attempts to use biological weapons. Professor Barry Kellman reports on Aum Shinrikyo:

> In April 1990, Aum attempted to attack the Japanese parliament with botulinum toxin aerosol. In 1992, Aum sent a mission to Zaire to assist

> in the treatment of the Ebola virus disease victims in order to find a sample of the Ebola strain to take back to Japan for culturing purposes. In June 1993, the cult tried to release poison at the wedding of the Japanese crown prince. Later that month, Aum attempted to spray anthrax spores from the roof of a building in Tokyo. All these attacks were unsuccessful and resulted in no casualties.[8]

Even though the cult's chemical weapons program proved to be deadlier, a well-equipped laboratory was found with various biological substances that were used to successfully cultivate bacteria and viruses.[9]

Since the World Health Organization (WHO) announced the eradication of smallpox in 1980, there has been a debate about whether the last remaining virus strains in laboratories should be destroyed. There has also been much discussion of the possibility of terrorist use, as humanity has become very vulnerable following the suspension of vaccination.[10] At present, the United States and Russia still have small stocks of smallpox strains, which are kept in highly secure laboratories. According to the WHO, no other laboratory has official access to the virus.[11] However, since the attacks of 11 September 2001 (9/11), the general debate on chemical, biological, radiological, and nuclear (CBRN) weapons has been broadened again to include other pathogens. This was also strongly reinforced by the anthrax letters sent only a week after the devastating al-Qaeda attacks. Of the 22 infected, 5 died. The perpetrator was, according to an FBI investigation, a professional Army biological researcher with access to all the essential materials.[12] Also in 2001, the book *Germs: Biological Weapons and America's Secret War* was published only a few weeks after 9/11 and remained at number one on the *New York Times* bestseller list for more than two weeks. It contained a number of investigative novelties about the United States' biodefense projects.

After 2001, it became known that al-Qaeda had already been pursuing a practical bioweapons program since the beginning of 1998. In 1999, the terrorist group recruited a Pakistani biologist to develop biological weapons in a laboratory in Kandahar. In 2001, a biochemist from the al-Qaeda network may have been able to isolate a lethal anthrax strain.[13] The actual progress of al-Qaeda's anthrax research was more advanced than global leaders suspected, but the group was never able to produce a viable bioweapon.[14]

In 2003, there was the first case of letters filled with ricin toxin in the United States. The perpetrator is unknown still today. Ricin toxin is a plant material, so there is no infection and reproduction as with microbes. Al-Qaeda terror cells in Great Britain, Spain, Italy, Turkey, Sweden, and Germany were also planning attacks with ricin toxin in 2003. Suspects were arrested in Great Britain, Spain, Italy, and France.[15] In 2004, ricin toxin contamination was detected in a building in Washington, DC. Until 2009, this was the last major incident involving material that could be used as a biological weapon, with a potential terrorist background.

Since then, there have been a number of incidents up to 2021 due to the relatively easy production of ricin toxin. Most of the recorded cases have occurred in the United States. The lethality of ricin toxin is illustrated by the example of Bulgarian dissident Georgi Markov, who was killed in an assassination in London in 1989 by only 0.2 milligram of the agent.[16] Significant incidents since 2009 include ricin letters sent to American politicians in 2013, ricin toxin in the hands of a right-wing militia in the United States, attempted orders via the darknet, and possession of ricin toxin in 2018 and ricin-powder-filled letters again in 2020.[17] The darknet is a variety of networks that are shielded or hidden from public access. The attempt by a jihadist living in Germany in 2018 to carry out an attack with ricin toxin stands out, as he was believed to have had contact with members of Islamic State and managed to produce potentially lethal ricin toxin on his own. He followed internet tutorials on how to make explosives and extract ricin toxin with rudimentary resources.[18] But also, in Iraq and Syria, the Islamic State tried to obtain functioning biological weapons. A laptop discovered in Syria in 2014 contained many different instructions for the construction, storage, and delivery of weapons of mass destruction.[19] However, the Islamic State's focus seemed to be on chemical weapons, especially after 2014.

A study by the U.S. National Consortium for the Study of Terrorism and Responses to Terrorism that was examining 74 nonstate actor incidents involving biological agents from 1990–2011 concludes that use of an agent, possession of a nonweaponized agent, and attempted acquisition are the most common events. Other categories not recorded as often include plot, interest, possession of a weapon, threat with possession, and attempted use of an agent. The most common types of perpetrators involved in attacks during the period studied are cults and lone actors.[20]

As in many other areas, the ongoing COVID-19 pandemic is also a turning point in the field of bioweapons. Since 2020, there have been a number of different scientific papers examining the link between COVID-19 and terrorism. Experts at University College London's Jill Dando Institute of Security and Crime Science found evidence as early as May 2020 that extremist groups were calling for the virus to be deliberately spread and to infect religious or ethnic groups particularly deemed adverse. Likewise, conspiracy theory narratives that SARS-CoV-2 was designed as a biological weapon became established.[21] The deliberate spread of SARS-CoV-2 was particularly discussed by parts of the American neo-Nazi scene, who set their sights on a violent collapse of the current system to establish a White ethno-state afterward. In right-wing Telegram channels, for example, the door handles of non-Whites, Jews, or FBI facilities were indicated as targets for the application of infectious saliva. Initially, the approach was also discussed in jihadist circles, as the Western states were most affected toward the beginning of the pandemic. In April 2020, an alleged Islamist was arrested in Tunisia for planning to deliberately spread SARS-CoV-2 among local security forces. In addition, many experts agree that COVID-19

has served as a great inspiration for various groups of different orientations that have already considered researching or acquiring biological weapons.[22] Various religious groups of different faiths see COVID-19 as a kind of revenge of God, without actively wanting to contribute to its spread.[23]

In summary, it can be said that, as with chemical weapons, the procurement or attempted procurement of dual-use equipment, which could potentially be used for biological weapons production, has increasingly shifted to the internet since 2009. Here too, in addition to the regular online shops, the so-called darknet is once again playing a prominent role. As a relatively easy-to-obtain toxin, ricin toxin has played an increasingly important role since 2009, and the motivations of nonstate actors have generally been diversified. However, ricin is more suitable for attacking individuals or small groups, since a large-scale attack in the open is logistically difficult and would not be very effective. A major attack with biological weapons predicted by some analysts before 2010 was not realized until the end of 2022. Effective weaponization of SARS-CoV-2 has been partially attempted, but it has not been measurably successful, as all attempts were under primitive conditions.

Warnings about antibiotic-resistant bacteria, vaccine resistant viruses, and the creation of completely new pathogens (chimeras) are also not new and were already voiced, for example, by the authors Tom Mangold and Jeff Goldberg in 1999. In their 1999 prediction, it will take about 20 years before genetic engineering can completely circumvent current biological countermeasures.[24]

The World in 2030

Clearly, the environment for an analysis of biological threats will be different by the year 2030. The author does not attempt to draw a coherent picture of the security world of the future, but rather to identify some factors that are important for the future biological threat environment. One is the overall geopolitical evolution of NATO's relationships with other state and nonstate actors. In a more cooperative world, the role of new treaties and their compliance in dual-use research and biological agents is an important variable of the future. In this context, the future monitoring and prevention of proliferation of pathogens for production and distribution is also an important factor. Another relevant factor is the political stability of countries with significant biotechnology research laboratories and stockpiles of potent pathogens. In the event of insufficient protection of the facilities or political unrest and upheaval, the hazardous materials could fall into the wrong hands.

Other factors are additional natural pandemics through 2030 and the long-term effects of COVID-19 on future strategic considerations within NATO, its member states, and among potentially hostile actors. The consequences of Russia's war of aggression, the following build-up of capabilities, shifts in foreign policy paradigms in some NATO countries, and a potentially more uncooperative international order will also play into the future of a biological threat environment. Add to this a huge number of potential black swan events, ranging

from doomsday cults to false flag attacks to extortionist criminal groups. Equally unpredictable, of course, are future conflicts and their associated events. The next section discusses a number of megatrends that, unlike the variables identified in this article, have already begun in the past and will continue to have a relatively reliable impact through 2030 and beyond.

Megatrends through 2030

Climate change as a megatrend through 2030 is having a significant impact on future biological threats. It has long been known that climate change will lead to a further geographic spread, as well as a net increase in transmissions of infectious diseases.[25] The Euro-Atlantic area in particular will be affected by new species emigrating from the south. The deliberate introduction of already found pathogens or vectors to new habitats farther north might be a terrorist method, made possible in part by climate change. At the same time, permafrost is thawing in many places, revealing frozen pathogens that might not be present today. For example, a child died in Siberia in 2016 from anthrax that was frozen in the permafrost, but smallpox and dangerous influenza strains can also potentially thaw in the Arctic region and be transmitted to humans. Similarly dangerous are much older and completely unknown pathogens that are buried several meters deep in the soil and could come to the surface by 2030.[26] Terrorist use is unlikely but not impossible. An additional factor, accelerated by climate change, is that in many cases natural disasters are followed by infectious disease outbreaks and epidemics. This is mainly due to displacement, which is mostly negatively connected to the availability of safe water and sanitation facilities, the degree of crowding, and the availability of health care services.[27] Another impact is that due to the decrease of global animal and plant biodiversity, large populations from one species potentially have advantages in dispersal in an imbalanced manner. Thus, insects and vectors used as bioweapons can more effectively attack plants, humans, and animals while transmitting and reproducing diseases.

Another set of megatrends such as population growth, migration, urbanization, and demographic change also interact with biological threats to NATO forces through 2030. Poor sanitary conditions in densely populated and rapidly growing megacities make the spread of pathogens more likely. NATO nations are experiencing steady demographic change that includes a rapidly growing older segment of society that is more vulnerable to many transmittable diseases.

Due to ongoing globalization and worldwide trade, especially online, it can be assumed that it will continue to be possible to order and deliver laboratory and medical equipment online through 2030. Similarly, pathogens can spread rapidly and potentially undetected in a short time due to the long-distance transport of people and animals.

The next megatrends identified by the author are inequality and poverty. However, meat consumption has often risen as a result of the greatly increased standard of living in China, for example. While total meat production in other

parts of the world has increased only slightly since 1990, the amount in Asia has doubled. But individual consumption has also risen sharply in China and Brazil since 1990, while individual consumption in many NATO member states has declined slightly since around 2010.[28] It should be noted that there is a clear link between infectious diseases and meat production.[29] In particular, inadequate hygiene and safety measures, as well as factory farming, contribute to new zoonotic viruses and epidemics.[30] Due to various reasons, including high meat consumption, experts suspect that several and more severe pandemics will follow in the future.[31] However, a significant decrease in global meat consumption is not expected. In addition, more meat consumption significantly increases greenhouse gas emissions, which in turn increases biological hazards associated with climate change. Local poverty and inadequate government resources will continue to contribute to the inability to contain and prevent local outbreaks of infectious diseases in a timely manner through 2030, potentially posing a threat to nations far away.

The next megatrend through 2030 is briefly discussed in terms of digitalization and technological advances. As described in more detail in the next section, advances in biotechnology and medicine, as well as in the field of bioinformatics, are already contributing to major breakthroughs in the manipulation of bacteria, viruses, and animals. Bioinformatics is an interdisciplinary science that uses computer-assisted methods to try to generate new findings in the fields of biotechnology and medicine. This trend is very likely to continue by 2030 and further breakthroughs may be recorded. In addition, the advanced methods already known today for manipulating and producing pathogens are expected to become cheaper, easier to use, and possibly more widespread by 2030. This depends on whether there will be stronger regulations in this area in the future. However, it is very likely that civilian research and genome databases with potent pathogens that are freely available on the internet will be expanded by 2030 and could still be misused. The internet also facilitates recruitment and communication between nonstate actors hostile to NATO. Just as today, by 2030 the internet will likely make it possible to communicate encouragement and support for the development or terrorist deployment of bioweapons regardless of location.

The final megatrend cluster identified by the author is hybridization and asymmetric warfare. Both trends pose a certain threat in a world in 2030 in which limited-use biological weapons can wreak havoc on the enemy, but not on the enemy's own forces. In addition, there is the possibility of concealing the origin of, for example, a local epidemic or the possibility of biological weapons that are not lethal to humans. In a hybrid conflict, an adversary actor could, for example, also want to cause economic damage or supply shortages and target livestock populations or agriculture. In a hybrid conflict, it would also be possible to use pathogens against NATO forces to incapacitate soldiers for a longer period of time without causing them permanent harm. In a possible future asymmetric conflict between now and 2030, it must be expected that

the facilitated production and delivery of limited biological warfare agents will allow a heavily outnumbered actor to pretend that it has the ability to establish a certain balance against a perceived superior adversary.

Overall, for the complex 2030 threat environment, a broad set of important variables and longer-lasting megatrends suggest that there are several indications that by 2030 the threat of deployment may be higher and the impact more severe. In the next section, special attention is given to emerging and disruptive technologies through 2030 that are important for the design, production, and delivery of potential biological weapons.

Emerging and Disruptive Technologies until 2030

This section of the article will outline how new technologies are having a major impact on biological weapons by 2030. Before analyzing specific technologies in more detail, however, the author first wants to point out that biological weapons not only have a purely military use, but also, like other weapons of mass destruction, have a particular impact on politics and society. With a large number of digital devices connected to the internet, online media, and the peculiarities of social networks, actors could use the threat or deployment of biological weapons to spread panic and fear. Allison E. Betus, Michael K. Jablonski, and Anthony F. Lemieux examine the important role of media in our increasingly digitalized world as follows:

> Violent acts initiate media coverage, as well as word-of-mouth transmission, functioning as a gateway that draws attention to the terror group and its messages in a manner that increases the salience of the communication; then media provides additional information contextualizing the original act. Media coverage may make the group initiating the communication look more dangerous or powerful than is warranted.[32]

It is thus becoming increasingly clear that CBRN threats are not only reflected in new hardware, but also increasingly affect the virtual information and communication space, as well as the public perception of a real or perceived threat.

A research paper by the NATO Centre of Excellence Defence Against Terrorism identifies a countervailing mechanism for the interaction of terrorism and technological progress. In general, military and civilian innovations influence each other with a reciprocal push and pull mechanism. This also benefits nonstate actors, who usually focus on adapting and refining existing and proven dual-use technology for their own purposes.[33] In addition to easy obtainable dual-use goods, high-tech equipment and material is mostly stolen from professional armed forces, bought on the black market, or supplied by state actors. In *NATO Strategic Foresight Analysis: 2017 Report*, one of six chapters is devoted exclusively to future technologies. The report describes, among other things, the rate of technological advances, the number of individuals with access to the internet, the potential of adversary non-state actors' access to new technologies,

the international interconnectedness, the amount of data collected, and an increase in the number of sensors in the world. At the same time, it is becoming more difficult for states, international organizations, or other frameworks to effectively regulate potentially dangerous technologies. This is due, among other things, to the rise of dual-use devices, effects of globalization, an increase in the power of the commercial sector, and the rapid pace of market maturity of new technologies, where democratic mechanisms can often be slow to react.[34]

The first tangible technologies under consideration are user friendly AI applications and web scrapers, which can already easily search large amounts of information about a certain online topic on the internet or in a database, for example about pathogens. AI can then theoretically analyze or even interpret the results. If no powerful computer hardware is available, capacity can be rented via cloud services. This intersection could well be classified as digital dual-use. The consequence is that gene combinations can be tested on the computer before they are cultivated. This saves time and resources and can be used to develop pathogens with specific properties. The process of producing a large number of molecules by combining and varying different chemical components using modern methods also exists in chemistry.

One of the most important future technologies described in this article are modern biological applications. These include genetic engineering, synthetic biology, and biochemistry. Again, this is an area of dual-use research. Genetic engineering is the direct genome manipulation of organisms, including clustered regularly interspaced short palindromic repeats (CRISPR) gene editing that is probably one of the most important scientific breakthroughs of recent times. Especially in the field of biological weapons and nonstate actors, this is a method that can be misused with serious consequences. The special advantage is that, compared to prior methods, it provides easier, cheaper, and more precise additions or removal of parts of the genome while the organism is alive. Thus, in the future, it will be reasonably easy to turn bacteria, viruses, fungi, plants, and humans into genetically modified organisms.[35] In general, this field is well researched and there are many publications available, as vaccines, for example, are also being developed using similar methods. For instance, a research paper on the synthesis of horsepox was published in 2017. Dr. Tom Inglesby, director of the Center for Health Security at the Johns Hopkins Bloomberg School of Public Health, sees this as increasing the risk of smallpox synthesis.[36] In the future, it is believed that despite often grave ethical concerns and attempted political regulation, research will continue to advance. It is often difficult to regulate and identify dual-use applications early enough. However, strategic considerations and scientific great-power competition also play into this technology, as China, in particular, has recently become known for advances in genetic engineering, which are often seen as ethically critical.[37]

One of the many different aims of synthetic biology is to produce synthetic cells (i.e., synthetic life). In 2019, a synthetic bacterium was created for the first time from an artificial sequence of genomes.[38] In this way, even very dangerous

bacteria could theoretically be created as if from a construction kit. Research is currently being done on this with the aim of producing a synthetic drug delivery platform.[39] However, viruses can also be transported and distributed by synthetic bacteria. Advances in synthetic virology are particularly relevant to this study. In the future, it is expected that any virus whose DNA/RNA (deoxyribonucleic/ribonucleic acid) is available can potentially be reverse engineered, bringing viruses that have been eradicated back into circulation. Currently, the National Library of Medicine has a large database called the National Center for Biotechnology Information Virus (NCBI Virus), which contains the genetic data of nearly all known viruses, as well as other microorganisms and mammals.[40] There is an important report by the U.S. National Academy of Sciences, commissioned by the U.S. Department of Defense in 2018, which describes three particularly dangerous scenarios of synthetic biology. In addition to the already described technique of reproducing viruses with genetic code from the internet, it also mentions the possibility of making bacteria resistant to antibiotics and the possibility of programming microbes in such a way that they slowly poison people through their metabolism. The last method could lead to death after a long time and thus disguise the crime. Much more difficult to implement, but theoretically possible, is a so-called gene drive that automatically spreads through the population, altering people's DNA.[41]

The field of biochemistry is also important, as research into, for example, metabolism processes in cells, signal molecules, or enzymes must also be considered in the effect of biological weapons. The exact impact of this area of research up to 2030 cannot be forecasted precisely, but it is certain that the impact will be significant.

A new development that could potentially have an impact on chemical and biological weapons is microreactors in the form of a continuous flow reactor. Fundamentally, the idea is to allow chemical reactions to take place in a very small device. Advantages compared to large reactors include scalability, on-site and on-demand production, as well as a high reaction yield.[42] The small reactors can be scaled up to almost any size, and expensive, large, and complicated synthesis facilities in batch reactor design are no longer necessary, as the cult Aum Shinrikyo once built them. A 2013 study, however, stresses that the use of microreactors for the production of chemical weapons is limited. Nevertheless, future technological advances may well enable a broader range of warfare agents.[43] Advances in micro-enzymatic reactors are also expected in the field of biology.[44] This could help future terrorists or state actors to produce small quantities of toxic agents in almost any place in the world without significantly putting themselves at risk during production. Although the implications are not yet well understood, the cultivation of pathogens could also benefit from the technology.

Current and future often dual-use developments in nanoscience also offer many overlaps with biological weapons and means of delivery. But not only potentially lethal applications are being developed; nanoscience also supports

modern material sciences, engineering, and production. For some years now, several armed forces have been researching machines frequently called nanobots. However, this often refers to insect-size unmanned aerial vehicles (UAVs), which does not correspond to the "nano" definition. Nevertheless, these bionic insects, which are often only 2–3 mm in size and are capable of flying, can, for example, deliver a highly potent poison unnoticed to many locations.[45] In a swarm, technical systems could be manipulated, disrupted, or destroyed. However, real nanobots (i.e., nano-size synthetic drug carriers) are also not unlikely in the future. For example, a group of Chinese researchers undertook the first successful tests for targeted tumor treatment in 2018.[46] On the other hand, such carriers could also be used for the targeted transport of viruses and toxins. Bacteria have been used as drug carriers for similar applications for some time now. Theoretically, however, it is also possible to manipulate unmodified or transgenic insects with the help of nanotechnology, for example to increase the effect of distributed biological warfare agents.[47]

Other applications of nanotechnologies are very small computers, which will be important for small means of delivery and monitoring of production of biological and chemical warfare agents.[48] In general, by 2030, nano-size technologies are expected to make the dual-use laboratory equipment needed for biological weapon production, among other things, cheaper, more effective, smaller, and more flexible.[49] In addition, future attacks with nanotubes may offer entirely new possibilities for disguising origin and lethality. A researcher at American University explains: "For example, nanotubes could be used to deliver only the lethal parts of the anthrax virus—without the signature protein that is recognizable to the immune system." The researcher identifies three main dangers in linking nanoscience and potential biological weapons. First, rudimentary nanotechnology labs are already available on the internet for under $500 USD. Second, the technology makes it easier and cheaper to produce, disguise, and transport biological warfare agents. And third, the technology is not sufficiently regulated, which could lead to an asymmetric arms race that threatens the overall strategic security of major countries.[50]

The dual-use problem in the CBRN sector, which has already been mentioned several times in this article, has been recognized for some time. For this reason, the informal multilateral export control regime known as the "Australia Group" has been in existence since 1985. It deals with dual-use technologies, which can be misused for the production of chemical and biological weapons, among other applications. The NATO countries and the European Commission are members, but Russia and China, for example, are not, which makes international control much more difficult. Nevertheless, the group offers expertise in identifying potential dual-use applications. Additionally, after 11 September 2001, there were great efforts to provide weaponizable research with guidelines and, in some cases, regulations. For example, after a research report on the synthetic production of a polio virus was published in 2002, the U.S. government set up a high-level advisory body to draw up guidelines against the terrorist use

of biological research.[51] *Biotechnology Research in an Age of Terrorism*, a comprehensive work on the state of the art at that time, was published in 2004.[52] In 2012, the book *Innovation, Dual Use, and Security* was published, in which, in addition to the biological risks, attention was also drawn to the potential chemical risks. It contains a 300-page in-depth overview of many intersecting issues.[53] In 2016, a case came to light in which a Chinese company exported a synthetic opioid called carfentanil unregulated to countries in the Euro-Atlantic area. However, this chemical is so potent that it has already killed several unknowing drug users. Terrorist use could not be ruled out.[54] This incident is exemplary for several substances and devices. Furthermore, on the Chinese state level, there have been concerns from some NATO member states in recent years. The country is pursuing civil-military integration in many scientific fields, often resulting in dual-use goods.[55] In 2021, the United States accused China of not clearly distancing itself from weaponizable research in the biological field:

> China continues to develop its biotechnology infrastructure and pursue scientific cooperation with countries of concern. Available information on studies from researchers at Chinese military medical institutions often identifies biological activities of a possibly anomalous nature since presentations discuss identifying, characterizing and testing numerous toxins with potential Dual Use applications.[56]

Other countries that the United States accuses of a possible dual-use biological weapons program are North Korea and Iran. Russia is accused of not having properly destroyed "BW items specified under Article 1 of its past BW program."[57] An increase in civil-military dual-use research in the CBRN field poses the risk of openly available knowledge being misused for malicious purposes. The next section will take a closer look at the actual level of research in 2023 and what developments are possible by 2030.

Possible Biological Threats by 2030

Without question, the biological threats of the future are increasingly severe. The individual threats are often incomprehensible for nonexperts, as biological warfare can be carried out by using viruses, bacteria, fungi, insects, or plants. Almost all animals are possible vectors, and in the far future, even mechanical products or highly manipulated organisms could also be possible vectors. In addition, synthetic biology, nanotechnology, and DNA manipulation open up a whole new range of possibilities for modifying or even completely rebuilding or recreating viruses and bacteria. The latter are called designer pathogens. These technological advances were foreseeable for some time, and yet they only came to public attention because of the global pandemic. But as complex and diverse as the possible types of biological weapons are, so are the techniques to enhance the efficacy of biological weapons through biological engineering. A 2013 report in the *Dartmouth Undergraduate Journal of Science* lists the possible techniques for weaponizing biological materials. These include the manip-

ulation of bacteria; the aforementioned designer pathogens; the destruction or replacement of individual genes in the context of misused gene therapy; stealth viruses that only unfold their effect in the body after external or internal activation; host swapping diseases that, for example, specifically jump from domestic cats to humans; designer diseases that, for example, cause artificial cancer; and personalized biological weapons. The latter spread approximately asymptomatically in the population and only have an effect on certain genetic characteristics of a person or group of people.[58]

In his 2002 contribution to *The Counterproliferation Papers* of the U.S. Air Force Counterproliferation Center at Air University, Michael J. Ainscough describes the threats that could become reality by 2030. Based on findings of the JASON Defense Advisory Panel in 1997, Ainscough describes six future threats. First, he talks about binary biological weapons that can be used for extortion or safe handling. For this, a harmless host bacterium and a virulent plasmid would be isolated separately and threatened with the release of the associated second component, which would then interact to produce its effect. As far as designer genes are concerned, the researcher concludes that these have long been state of the art with simple modifications at the time of the study. Future designer pathogens will have far more complex capabilities and will be able to exhibit a whole range of modified characteristics. Regarding gene therapy, he writes:

> There are two general classes of gene therapy: germ-cell line (reproductive) and somatic cell line (therapeutic). Changes in DNA in germ cells would be inherited by future generations. Changes in DNA of somatic cells would affect only the individual and could not be passed on to descendants. Manipulation of somatic cells is subject to less ethical scrutiny than manipulation of germ cells.[59]

Already 25 years ago, viruses were used as vectors to insert genes into mammalian cells. This genetically engineered virus was successfully used to prevent rabies in wildlife. Likewise, viruses were successfully used as vectors for mousepox viruses 25 years ago. This allowed vaccination of mice to be circumvented, which died shortly afterwards. The concept of stealth viruses is not new in nature. In this case, an initially unnoticed virus could enter human cells and wait for an external or internal signal. One related example are oncogenes, which are mutated genes that cause cancer as soon as they are activated. Some viruses have segments of DNA that mimic oncogenes. Other substances, bioregulators, physical processes, or external influences such as ultraviolet light could thus activate the virus. Ainscough also writes about host-swapping diseases and designer diseases. In the future of 2030, it could be possible to create the suitable pathogens for a certain disease pattern. This would make it possible, for example, to temporarily shut down the immune system or induce cell death in certain cells.[60] Twenty years later, Ainscough's prognoses are all proving to be increasingly technically feasible. Except for complex designer pathogens and diseases, all predictions are applicable in the year 2023.

Although some of the possible applications mentioned have not yet been achieved in practice, thanks to the aforementioned CRISPR-Cas9 gene-editing technology and the general progress in the field, it is only a matter of time before the biological weapons mentioned are successfully tested within military or civil dual-use research. Another extremely problematic aspect is that CRISPR is not a high-tech technology that is only available in secure laboratories. At the current rate, it is foreseeable that in the world of 2030, manipulated and synthetic biological substances could take on an almost everyday character. But how difficult is it really for future actors to actually develop and deploy one of these methods themselves?

Based on the state of the art in 2015, researcher Zian Liu of the University of California, Berkeley, concludes that there are five potential barriers that could prevent nonstate actors without access to professional laboratories from creating novel biological weapons. First, it is not easy to create a properly protective research environment that will secure the actor adequately. Secondly, although it is possible to order all the necessary materials on the internet, very specialized equipment for very dangerous substances and many test runs cost up to $30,000 USD. If an already dangerous bacteria or virus strain are used as an initial substance, a screening of the person placing the order is usually requested. However, there are sometimes great differences in this respect worldwide. Nevertheless, there are already mechanisms that automatically subject the online ordering of several suspicious materials to a closer examination. An example is the code of conduct for gene synthesis published by the International Association of Synthetic Biology in 2009. Fourth, it is often standard practice to modify existing research for one's own purposes. However, specific research on modern biological weapons is of course top secret. But it is still possible to gather information from civilian dual-use literature, but this requires a higher degree of specialist expertise. Fifth, the actor would have to undertake potentially extensive testing and adjustments prior to deployment. Such tests can easily arouse suspicion in various ways. The author also describes that there is already an established community of so-called biohackers in many countries around the world. Determined nonstate actors might join such an often anonymous internet hobby community to act more effectively.[61]

At the same time, of course, it is also possible that such a biohacker could lose control of a potentially dangerous agent as a result of an accident, since generally weaker standards of safety are observed in amateur labs. Liu's six-year-old remarks must also be seen in the light of the fact that more advanced technologies are already available on the internet now. In the future, it will probably be even easier to circumvent the barriers as, for example, the aforementioned small flow reactors and CRISPR-Cas9 applications become widely marketable.

All in all, synthetic or DNA-engineered biological weapons can potentially cause enormous damage, but a closer look reveals that, at least for nonstate actors, production is currently not as easy as it might seem. By 2030, however, some of the current barriers are expected to be significantly lower. Although it

is possible to learn the fundamentals via internet courses, in most cases a solid academic education is needed to gain practical experience with the laboratory equipment. Compared to genetically modified agents, existing natural pathogens may pose an even greater danger, as slightly less experience is required to weaponize them. There is also more publicly available research and potential natural source sites for such pathogens. In 2014, for example, a Tunisian jihadist did not even attempt to produce complicated pathogens, but instead records were found on their laptop of how the causative pathogen of plague (*Yersinia pestis*) can be isolated from infected animals and subsequently weaponized. The chemist and physicist would presumably have had the theoretical prerequisites for creating his own strain, but it seems the costs were too high compared to the benefits.[62] He was caught without carrying out an attack.

It would also be relatively easy for nonstate actors to take advantage of a natural outbreak to infect themselves and then infect as many other people as possible. Breaking an imposed quarantine during a disease outbreak for political reasons could also be classified as terrorism, as people could be killed indirectly. Such intentions, as well as acting as a so-called superspreader, are entirely possible, as already described in the section on SARS-CoV-2. However, it is relatively difficult to deliberately infect oneself with a naturally occurring virus as the first carrier. Another comparatively simple biological weapon that could be used for attacks in the future is the mass breeding of insects. This can lead to effective attacks on crops, but as soon as the insects are to be used as vectors for diseases against humans, a greater effort might be required, although it might still be much less than that of producing a synthetic pathogen. The use of insectoid vectors proved to be very effective in the operations carried out by the Japanese during the Second World War. Other biological agents already used in the past, such as anthrax and ricin toxin, might also potentially be used in the future again. Currently, the Centers for Disease Control and Prevention lists more than 20 dangerous bioterrorism agents, which they subdivided into three categories.[63]

In addition, there is the danger of developments by state actors that could be misused for terrorist purposes by employees, fall into the hands of nonstate actors, be released as a result of an accident, and could be used intentionally or as part of a covert operation. The unconfirmed efforts of the People's Republic of China operating a disguised dual-use bioweapons program are a cause for concern.[64] It is also very problematic that various states have not ratified international agreements and, in some cases, do not adhere to international standards, which could facilitate proliferation to potentially adversarial nonstate actors. The internet, and its global expansion, will continue to play a fundamental role in the future through legal and illegal orders, educational courses, and specialized biohacking communities, as well as the latest research and publicly accessible DNA/RNA databases.

With a prospective application in mind, a distinction must be made between how demanding it is to produce or obtain a specific biological weapon.

As with chemical weapons, greater effectiveness goes mostly hand in hand with more difficult acquisition and are thus less likely to be used. This rough prediction may be obsolete by 2030, as technological advances lower the threshold for acquisition while increasing lethality. As emphasized in the introduction, it is important to note that various current and future biotechnological developments have the potential to limit and thus to a certain degree control transmissible biological weapons.

Current and Future Means of Delivery for Biological Material

Due to the often-unstable nature of biological pathogens outside the laboratory, methods of dissemination are also important. In the following, current and conceivable methods by 2030 are examined in more detail. A whole range of bombs, including cluster bombs and balloon bombs, were developed for use with biological weapons at the beginning of the Cold War. Many of these developments were aimed at destroying enemy crops with plant pathogens. In the Second World War, Japan used, among other things, ceramic bombs filled with pathogens. While most chemical weapons can be stored for longer periods of time in their means of delivery and can be used relatively effectively by many methods, biological weapons usually require a much more cumbersome procedure. Due to the high impact energy of nonbraked bombs and missiles, successful dissemination of a biological agent is not likely. Parachuted bombs with a large-scale dispersal mechanism are more likely to succeed. However, anthrax spores are nevertheless known to survive dispersal by low-yield explosion, as found for example in the American E61, E120 or M143 cluster bomb submunitions developed in the 1960s.[65] However, a careful explosive delivery system for sophisticated bioweapons is very difficult for nonstate actors to achieve on their own. A civilian aircraft could be bought or rented for the drop of a bomb or cannister, but the overall cost of such a venture is very high compared to the possible outcome.

Easy to control, maneuverable, low-cost UAVs with a comparatively high payload designed for the civilian market have become quite popular in the last decade and see regular combat operation, for example in the Ukraine war of 2022. In addition, camera technology is becoming smaller and smaller, batteries come with improved storage capacity, and small and lightweight flight controllers, accelerometers, and GPS (Global Positioning Systems) are becoming increasingly widespread. Thanks to mass production, mostly in the People's Republic of China, models are now available in many price ranges and payload sizes. In the meantime, a large market has also established itself with do-it-yourself components with which mission-oriented UAVs can be built relatively easily. This can be done both as a fixed-wing aircraft and as a multicopter or helicopter. In recent years, a growing market has also emerged that specializes in professional applications and offers more expensive, but still affordable, products. In the United States alone, almost 750,000 commercial and recreational drones

are currently registered.[66] At the same time, effective defense against these commercial UAVs remains a major challenge. In practice, it is also difficult to distinguish between registered and legal drone flights and potential attacks.

At an event organized by the Center for Arms Control, Energy, and Environmental Studies in 2011, some interesting points were made in relation to UAVs. For example, a simulation was mentioned in which 900g of weapons-grade anthrax would be released 100 meters above a large city. With appropriate winds, about 1.5 million people would be infected and tens of thousands would die despite strong containment measures. At the same event, the TAM-5 model aircraft was mentioned, which flew automatically for 39 hours in 2003 and traveled more than 3,000 km over the Atlantic.[67] Since 2009, more and more UAVs have been configured as multicopters. These models usually cannot fly as far or as long as fixed-wing aircraft, but they are more maneuverable and usually easier to operate. Modern remote-controlled aircraft can fly far faster than 500 km/h; modern quadrocopters far faster than 200 km/h. For professional applications, there are now drones with a payload of more than 100 kg.[68] In 2016, British prime minister David Cameron warned that UAVs could disperse radioactive material in massive quantities over cities. He is probably alluding to the wide availability of automated crop duster UAVs, which are in fact a low-effort, high-impact means of delivery for terrorists, especially when many people are crowded together in the open. Instead of radioactive material, however, chemical or biological material could be effectively disseminated.[69] State actors with access to professional technologies have resources to develop further technical solutions tailored to the agent. Manned aircraft for the deployment of CBRN material have been little considered by nonstate actors. In the past, Aum Shinrikyo tried to modify a Mil Mi-17 helicopter to spray toxic gas over Tokyo.[70] In 2001, an al-Qaeda terrorist traveled to the United States to possibly prepare an attack with a crop duster plane.[71]

In addition to aerial deployment, CBRN material can also be deployed from the ground. The direct application of pathogens, as in the 1984 Rajneeshee bioterror attack, can be considered a ground-based attack. The same applies to attempts to deliberately transmit SARS-CoV-2 or other viruses to, e.g., door handles or from person to person. This category also includes assassinations with biological warfare agents.

A subcategory of biological warfare is entomological warfare. There are two fields of application, because insects can be used to act directly as weapons or to spread pathogens. But noninsectoid animals can also be used to deliberately spread pathogens. This type of warfare was first systematically studied and applied during the Second World War. Japan was particularly involved; the empire infected Chinese populations with plague-infected fleas and cholera-spreading flies. This mode of transmission proved catastrophically effective. Yellow rats were also bred in large numbers for use as vectors.[72] After the war, the Soviet Union, among others, researched ticks as vectors. According to their own statement, an automatic insect breeding facility was developed.[73] Such a

facility was also planned in the United States, where mosquitoes and fleas were successfully tested as vectors and were dropped from airplanes.[74] But nonstate actors have also recognized the advantages of insects as biological weapons. For example, in 1989, after a letter from a group called "the Breeders" was found, "peculiar patterns of Mediterranean fruit fly infestation in southern California that year" were detected.[75] More recent cases have not been detected. In principle, it is easier to use insects as weapons than to successfully infect vectors with deadly diseases without endangering oneself. Major financial damage or famine due to crop shortfalls can be a consequence that is not directly fatal to humans.

As already indicated, the biological field is probably the most significant for the future. The possibilities of releasing and spreading a fully developed pathogen are very diverse and almost impossible to prevent. In jihadist circles, for example, one of the terrorists could be the first carrier, while other types of terrorists might want to harm a specific person or group of people. From poisoned water to public salad buffets, there are many methods. In the future, however, genetically manipulated or even synthetic bacteria, insects, or other animals will be particularly useful as vectors. Such animals can be bred or designed according to the requirements at hand (e.g., to reproduce and spread particularly quickly or to deliver the pathogen particularly effectively). Similarly, in the future it will often be difficult to distinguish manipulated animals from nonmanipulated animals. Thus, the origin of the outbreak can be concealed, which presents potential for a state attack disguised as a terrorist attack, or vice versa.

Biological means of delivery of pathogens can already be prepared with the help of artificial hatcheries or programmed to reproduce themselves as quickly as possible. The latter might be a logistically more effective solution, although manual incubation requires less expertise in the field of molecular biology. In the future, modified organisms may be able to identify and attack certain people or groups of people on the basis of certain characteristics or infect them specifically with the transported pathogen. Similarly, carrier animals could be manipulated to feel comfortable in other climates or environments and attack the local population or displace native species. Climate change would accelerate such intentions. It is also possible that by 2030, technologies will exist that can artificially control insects or small animals, turning them into covert weapons. Currently, this already works with beetles. In this way, CBRN materials could be delivered unnoticed to a specific target without attracting attention. A pathogen that has a deliberately long delay to disease onset or death built in can be used to spread unobtrusively in humans or animals before it is detected.

In addition to the ways of delivering biological material already discussed, there are other ways that can be used to contaminate soil, water, or plants. The perpetrator can either use one of the previously explained systems, such as an agricultural UAV. A simpler way is to distribute the agent personally in unguarded places. Biological agents such as anthrax are likely to contaminate soil permanently. The two best-known examples are Gruinard Island in Scotland and Vozrozhdeniya Island in what is now Uzbekistan and Kazakhstan.

Both were partially contaminated by tests with *Bacillus anthracis*, the cause of anthrax; studies proved the extreme persistence of the biological weapon in soil during initial decontamination attempts.[76] To alert the public to the dangerous situation on the island, unknown perpetrators sent two packages of soil samples from Gruinard Island almost 40 years after the initial release of anthrax agent. One of the packages actually contained anthrax spores.[77] The island was then thoroughly decontaminated. The former Soviet biological weapons test site in the Aral Sea was also decontaminated in 2002 with funds from the United States, because many anthrax cultures were not sufficiently destroyed by the Soviets. Nevertheless, it is likely that live spores could still be found in unknown locations on the island. *Yersinia pestis*, known as plague, and smallpox virus have also been experimented with on the Soviet testing area but are not likely to have survived until today.[78]

The deliberate poisoning of water, mostly of human drinking water, has been discussed many times in the past. In such a case, it is known as a point source. In fact, in 1972, two teenagers tried to poison Chicago's drinking water with biological agents, but they did not come close to achieving their goal.[79]

The deliberate poisoning of plants or livestock with biological agents is a very broad field of application that has been studied and partially applied since before the Second World War. In the past, Germany, France, Japan, Iraq, the United Kingdom, the United States, and the Soviet Union pursued such programs, sometimes on a large scale.[80] The means of delivery are either vectors or insects themselves, but the use of anticrop fungi and other transmissible plant diseases has also been successfully tested. Once applied to a plant, it then serves as both the means of delivery and the target of the weapon. As with soil contamination, there are theoretically multiple motivations for terrorists to engage in agro-terrorism. Agro-terrorism can often be closely linked to entomological warfare methods. For more information, see the section on animals as a means of delivery. Jonathan Ban of the Chemical and Biological Arms Control Institute lists some motivations:

> Some actors may be motivated for the same reasons as other terrorist actions—to attract attention to a cause, incite fear, disrupt society, or demonstrate a capability with the intent of exacting political concessions. Other actors may be prompted by different motives—economic interest, sabotage, or revenge.[81]

He lists several cases in which crop poisoning was threatened or carried out. In the described cases, chemicals like mercury or cyanide were used for poisoning, but not self-transmitting biological weapons. Also, the alleged medfly attacks in California in 1989 had food production, in this case mass-produced fruits, as a target.[82] The Federation of American Scientists provides information on further incidents of biowarfare against agriculture: "In 1985 and 1988, Iraq conducted field tests of wheat cover smut to demonstrate its effectiveness as an anti-crop agent. Iraq also produced canisters designed to disperse the fungal

agent over Iranian wheat fields. In Sri Lanka in the early 1980s, a group of Tamil separatists threatened to spread non-endemic plant diseases among rubber and tea plantations in a scheme to undermine the government."[83]

In the section on emerging technologies, the potential and current areas of application of nanotechnology in the CBRN sector have already been outlined. There is also a future field of application in the area of means of delivery. Future systems can use the bionic advantages of real living beings and combine them with the advantages of technical applications. Since only a few grams of various toxins or pathogens are often needed to have a lethal effect or to start an epidemic compared to current nuclear weapons, for example, nanorobots are also suitable for delivering the material. Also, camouflage as, for example, a mechanical rat or bird is possible to outsmart security measures of military premises or essential personnel. It is unlikely that nonstate actors will be able to build and operate such complex military high-tech means of delivery, but a dual-use application of such technologies is not impossible by 2030.

Fully autonomous vehicles are certainly part of the future of 2030. With autonomous UAVs, the damage of even low-quality CBRN weapons can be increased by automatically matching and selecting between multiple detected targets. Reprogramming requires IT skills, but these can also be obtained by terrorist groups. Deployed en masse, autonomous vehicles can carry out many different conceivable types of attacks and cause increased panic among the population, which is further exacerbated by the use of CBRN material. Autonomous drones can also target, for example, crowds of people with CBRN material, move on, and attack new identified targets. This saves CBRN material and makes the attack more effective, as even agricultural drones have a rather limited capacity when it comes to creating a deadly concentration of an agent in the air.

Possible Actors

The last and final section provides an overview of possible actors up to the year 2030. Earlier in the article, China and its dual-use biotechnology activities were discussed in more detail. Of the potentially hostile state actors, however, North Korea must also be mentioned, whose possible bioweapons program is explained in two reports as well as the Russian Federation, about whose current bioweapons allegations there is also a detailed article.[84] In the case of both countries, however, there is no definitive evidence. On Iran and a possible bioweapons program, sources are comparatively sparse.

Starting with state actors that may have sophisticated and resource-intensive capabilities to research, produce, and deploy biological weapons, it must never be forgotten that former state actors, like defectors or disloyal soldiers, may also get their hands on these biological weapons or sophisticated weapons get stolen or lost. In today's world and the world of 2030, there are also pseudo-nonstate actors who ostensibly operate autonomously but are significantly supported by a state actor. In addition to economically, religiously, and politically motivated

actors, there are also cults that stand out from other groups in the field of nonstate actors, since their goal may well be the extermination of all human life without limitation. Other nonstate actor groups that could theoretically plan to use biological weapons by 2030 are ecoterrorists, extreme conspiracy theorists, cyberterrorists, internal staff, renegade scientists, or laboratory security personnel. The third major category is unintentional accidents in laboratories or accidents involving members of the biohacker community at home. For example, at least two accidents occurred in coronavirus laboratories in China in 2004, and the local outbreak of foot and mouth disease in the UK in 2007 was traced to a laboratory in Surrey.[85] The fourth category is incidents, outbreaks, and attacks of unknown origin, which is not unlikely in the context of possible hybrid warfare by 2030.

Conclusion and Overall Threat Potential

In conclusion, NATO forces will find themselves in an increasingly dangerous biological threat environment by 2030. Despite the diverse threat environment, the alliance must credibly ensure that it can continue to operate actively in the aftermath of biological weapons attacks. Despite the high potency of biological agents, the issue is often treated only half-heartedly in armed forces and often remains a secondary consideration in national security strategies, despite the COVID-19 pandemic as an illustrative example. This article shows that there are virtually no limits to future biological weapons. This type of weapon of mass destruction has the potential to fundamentally change the future of warfare. As Ainscough's prognosis shows, this is not necessarily a new conclusion. The hypothesis is thus confirmed, although it is clear that forecasts for the future are always merely educated assumptions and that a large number of unknown factors play a decisive role in the real outcome.

It is very difficult to quantify the threat of future bioweapon attacks on a scientific basis. At the end of 2022, there is no concrete evidence that any actor is planning or threatening to use biological weapons in the near future. Nevertheless, the threat environment is evolving in a direction that fundamentally increases biological threats. Likewise, the progress of biotechnology will sooner or later lead to the development of limited transmissible bioweapons. So far, uncontrolled spread has deterred actors from using transmissible bioweapons. If, by 2030, it is possible to effectively limit biological weapons or make them nonlethal and endow pathogens with individual capabilities and attributes as designer pathogens, biowarfare could indeed establish itself as an alternative to traditional types of kinetic warfare in the future.

NATO forces must work closely together to develop effective counterstrategies and stay at the forefront of research to identify threats and develop effective countermeasures, as stated in the *NATO 2030* agenda. Additionally, the U.S. Marine Corps should address biological threats more thoroughly. At the same time, the defensive nature and safe conduct of their own biological research must always be made clear at the international stage and a treaty structure

adapted to the changed conditions of our time, in particular with the People's Republic of China, must be sought diplomatically. It must be reliably ensured that, despite a lower barrier, the use of biological weapons will continue to elude the interest of any actors in the future.

For further research, the author recommends the development of effective counterstrategies to future biological weapons attacks and an outlook on what biotechnological advances potential adversaries could use to make their soldiers more capable and resilient in the future.

Endnotes

1. *Force Design 2030* (Washington, DC: Headquarters Marine Corps, 2020).
2. Jason Blessing, Katherine Kjellström Elgin, and Nele Marianne Ewers-Peters, eds., *NATO 2030: Towards a New Strategic Concept and Beyond* (Washington, DC: Henry A. Kissinger Center for Global Affairs, Johns Hopkins University, 2021).
3. Kate Charlet, "The New Killer Pathogens: Countering the Coming Bioweapons Threat," *Foreign Affairs* 97, no. 3 (May/June 2018): 178–85.
4. George W. Christopher et al., "Biological Warfare: A Historical Perspective," *Journal of the American Medical Association* 278, no. 5 (1997): 412–17.
5. Matthew Meselson, "The Sverdlovsk Anthrax Outbreak of 1979," *Science* 266, no. 5,188 (1994): 1,202–8, https://doi.org/10.1126/science.797370.
6. Michael J. Ainscough, *Next Generation Bioweapons: The Technology of Genetic Engineering Applied to Biowarfare and Bioterrorism*, Future Warfare Series 14 (Maxwell Air Force Base, AL: Air University, 2002).
7. James Weaver, letter to the editor, "Slow Medical Sleuthing," *New York Times,* 24 April 2001.
8. Barry Kellman, "Biological Terrorism: Legal Measures for Preventing Catastrophe," *Harvard Journal of Law and Public Policy* 24, no. 2 (2001).
9. Kellman, "Biological Terrorism."
10. "Smallpox as a Biological Weapon," *Journal of the American Medical Association* 281, no. 22 (1999): 2,127–37, https://doi.org/ 10.1001/jama.281.22.2127.
11. "Smallpox," World Health Organization, accessed 11 May 2023.
12. "U.S. Officials Declare Researcher Is Anthrax Killer," CNN, 6 August 2008.
13. Rolf Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?* (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010).
14. "Al Qaeda's Bio Weapons," CBS News, 31 March 2005.
15. Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat*.
16. "Ricin and the Umbrella Murder," CNN, 23 October 2003.
17. "Two Georgia Men Convicted in Ricin Plot Against U.S. Government," Reuters, 17 January 2014; "*Breaking Bad* Fan Jailed over Dark Web Ricin Plot," BBC, 18 September 2015; "Henderson Man Sentenced for Unlawfully Possessing Ricin," press release, U.S. Attorney's Office, Eastern District of Texas, 2 August 2018; and Clare Hymes, "Woman Accused of Sending Ricin Letters to White House Charged with Making Threats Against the President," CBS News, 22 September 2020.
18. Florian Flade, "The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror," *CTC Sentinel* 11, no. 7 (August 2018).
19. Harald Doornbos and Jenan Moussa, "Found: The Islamic State's Terror Laptop of Doom," *Foreign Policy*, 28 August 2014.
20. "Ricin Letters Mailed to President and Senator," START, April 2013.
21. Nadine Salman and Paul Gill, "Terrorism during the COVID-19 Pandemic," UCL JDI Special Series on Covid-19: No. 13, May 2020.

22. Gary Ackermann and Hayley Peterson, "Terrorism and COVID-19: Actual and Potential Impacts," *Perspectives on Terrorism* 14, no. 3 (2020): 59–73.
23. Arie W. Kruglanski et al., "Terrorism in Time of the Pandemic: Exploiting Mayhem," *Global Security: Health, Science and Policy* 5, no. 1 (2020): 121–32, https://doi.org/10.1080/23779497.2020.1832903.
24. Tom Mangold and Jeff Goldberg, *Plague Wars*: *The Terrifying Reality of Biological Warfare* (New York: St. Martin's Press, 2001), 92.
25. C. Drew Harvell et al., "Climate Warming and Disease Risks for Terrestrial and Marine Biota," *Science* 296, no. 5,576 (June 2002): 2,158–62, https://doi.org/10.1126/science.1063699.
26. Amelie Bottollier-Depois, "How Climate Change Could Expose New Epidemics," Phys.org, 16 August 2020.
27. Isidore K. Kouadio et al., "Infectious Diseases Following Natural Disasters: Prevention and Control Measures," *Expert Review of Anti-Infective Therapy* 10, no. 1 (2012): 95–104, https://doi.org/10.1586/eri.11.155.
28. Hannah Ritchie, "Which Countries Eat the Most Meat?," BBC, 4 February 2019.
29. Romain Espinosa, Damian Tago, and Nicolas Treich, "Infectious Diseases and Meat Production," *Environmental and Resource Economics*, no. 76 (2020): 1–26, https://doi.org/10.1007/s10640-020-00484-3.
30. Laura Spinney, "Is Factory Farming to Blame for Coronavirus?," *Guardian*, 28 March 2020.
31. Bhaskara Reddy and Milton Saier Jr., "The Causal Relationship between Eating Animals and Viral Epidemics," *Microbial Physiology* 30, no. 1 (2020): 2–8, https://doi.org/10.1159/000511192.
32. Allison E. Betus, Michael K. Jablonski, and Anthony F. Lemieux, "Terrorism and Intergroup Communication," Oxford Encyclopedia of Communication, 26 October 2017, https://doi.org/10.1093/acrefore/9780190228613.013.409.
33. Afzal Ashraf and Anastasia Filippidou, *Terrorism and Technology* (Ankara, Turkey: Centre for Excellence Defence Against Terrorism, n.d.), 8.
34. "Allied Command Transformation Strategic Foresight Work," NATO, accessed 3 May 2023, 45–55.
35. Rasmus O. Bak, Natalia Gomez-Ospina, and Matthew H. Porteus, "Gene Editing on Center Stage," *Trends in Genetics* 34, no. 8 (2018): 600–11.
36. Kim Riley, "Bioterrorism Threats Require Common Global Experimentation Oversight, Expert Says," Homeland Preparedness News, 10 August 2017.
37. David Lawrence, "Genetic Engineering and Human-Animal Hybrids: How China Is Leading a Global Split in Controversial Research," Conversation, 3 September 2019.
38. Julius Fredens et al., "Total Synthesis of *Escherichia coli* with a Recorded Genome," *Nature* 569, no. 7,757 (2019), 514–18.
39. Pinero-Lambe et al., "Programming Controlled Adhesion of E. coli to Target Surfaces, Cells, and Tumor with Synthetic Adhesins," *ACS Synthetic Biology* 4, no. 4 (2014): 463–73, https://doi.org/10.1021/sb500252a.
40. "NCBI Virus," National Library of Medicine, accessed 11 May 2023.
41. Ian Sample, "Synthetic Biology Raises Risk of New Bioweapons, US Report Warns," *Guardian*, 19 June 2018.
42. Claire Delacour, "Why Use a Microreactor for Chemical Processes?," European Training Network for Continuous Sonication and Microwave Reactors, accessed 3 May 2023.
43. Andreas Zaugg, Julien Ducry, and Christophe Curty, "Microreactor Technology in Warfare Chemistry," *Military Medicine Science* 82, no. 2 (2013): 63–68, https://doi.org/10.31482/mmsl.2013.009.
44. Anita Salic and Bruno Zelic, "Synergy of Microtechnology and Biotechnology: Microreactors as an Effective Tool for Biotransformation Processes," *Food Technology & Biotechnology* 56, no. 4 (2018): 464–79.
45. Gary Sheftick, "Army Developing Robotic Insect," U.S. Army, 17 December 2014.

46. Suping Li et al., "A DNA Nanorobot Functions as a Cancer Therapeutic in Response to a Molecular Trigger in Vivo," *Nature Biotechnology* 36, no. 258–64 (2018): https://doi.org/10.1038/nbt.4071.
47. Jeff Daniels, "Mini-nukes and Mosquito-like Robot Weapons Being Primed for Future Warfare," CNBC, 17 March 2017.
48. "DARPA Microsystems Exploration Seeks Revolutionary Advances in Military Embedded Computing Technologies," Military and Aerospace Electronics, 16 July 2019.
49. Margaret E. Kosal, "The Threats from Nanotechnology," *Bulletin of the Atomic Scientists* 75, no. 6 (2019): 290–94, https://doi.org/10.1080/00963402.2019.1680054.
50. Nicholas Winstead, "The Applications and Implications of Nanotechnology," American University, 15 April 2020.
51. Erika Check, "Terror Watchdog Set up for 'Dual Use' Biology," *Nature* 428, no. 109 (2004): https://doi.org/10.1038/428109a.
52. *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press, 2004).
53. Jonathan B. Tucker, ed., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge, MA: MIT Press, 2012).
54. Erika Kinetz and Desmond Butler, "Chemical Weapon for Sale: China's Unregulated Narcotic," *Berkshire (MA) Eagle*, 7 October 2017.
55. Meia Nouwens and Helena Legarda, "China's Pursuit of Advanced Dual-use Technologies," International Institute for Strategic Studies, 18 December 2018.
56. *Adherence and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments* (Washington, DC: Department of State, 2021).
57. *Adherence and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments*.
58. Mackenzie Foley, "Genetically Engineered Bioweapons: A New Breed of Weapons for Modern Warfare," *Dartmouth Undergraduate Journal of Science* (Winter 2013).
59. Ainscough, *Next Generation Bioweapons*.
60. Ainscough, *Next Generation Bioweapons*.
61. Zian Liu, "Bioweapons . . . for Dummies?," *Bulletin of the Atomic Scientists*, 28 September 2015.
62. Bruce Goldman, "How-to Manual for Making Bioweapons Found on Captured Islamic State Computer," *Scope*, 3 September 2014.
63. "Bioterrorism Agents/Diseases," Centers for Disease Control and Prevention, accessed 4 May 2023.
64. Elsa B. Kania and Wilson Vorndick, "Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare'," Defense One, 14 August 2019.
65. Jeanne Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism* (New York: Columbia University Press), 101.
66. Federica Laricchia, "Consumer and Commercial Drones Worldwide—Statistics and Facts," Statista, 20 April 2022.
67. Eugene Miasnikov, *The Threat of the Use of Small UAVs by Terrorists: Technical Aspects* (Moscow, Russia: Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2004).
68. "Griff 300 Review: Drone that Can Lift 500 Pounds," Drone Tech Planet, accessed 4 May 2023.
69. David Hambling, "Could ISIS Really Attack the West with a Dirty Drone?," *Popular Mechanics*, 8 April 2016.
70. Suzuki Nathie, "Prophet of Terror: The Story of Shoko Asahara, Aum Shinrikyo, and the Danger of Religious Terrorism," *Suzuki's Thoughts* (blog), 14 January 2019.
71. Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat*, 16.
72. Jeffrey A. Lockwood, "Insects: Tougher than Anthrax," *Boston Globe*, January 2010.
73. Jonathan Ban, *Agricultural Biological Warfare: An Overview* (Alexandria, VA: Chemical and Biological Arms Control Institute, 2000), 3.
74. William H. Rose, *An Evaluation of Entomological Warfare as a Potential Danger to the*

United States and European NATO Nations (Dugway, UT: U.S. Army Dugway Proving Ground, 1981).

75. Ban, *Agricultural Biological Warfare*, 4.
76. Zaria Gorvett, "The Deadly Germ Warfare Island Abandoned by the Soviets," BBC, 28 September 2017.
77. "Biological Warfare: Dark Harvest," *Time*, 9 November 1981.
78. Zaria Gorvett, "The Deadly Germ Warfare Island Abandoned by the Soviets."
79. Michael Miner, "The Terrorist Mind—A Look Back at a 1972 Plot to Poison," *Chicago Reader*, 25 September 2012.
80. Ban, *Agricultural Biological Warfare*.
81. Ban, *Agricultural Biological Warfare*.
82. Ban, *Agricultural Biological Warfare*.
83. "Biowarfare Against Agriculture," Case Studies in Agricultural Biosecurity, accessed 4 May 2023.
84. Hyun-Kyung Kim, Elizabeth Philipp, and Hattie Chung, "North Korea's Biological Weapons Program: The Known and the Unknown," Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2017; Elisa D. Harris, *North Korea and Biological Weapons: Assessing the Evidence* (Washington, DC: Stimson Center, 2020); and Robert Petersen, "Fear and Loathing in Moscow: The Russian Biological Weapons Program in 2022," *Bulletin of the Atomic Scientists*, 5 October 2022.
85. Robert Walgate, "SARS Escaped Beijing Lab Twice," *Genome Biology*, no. 4 (2004): https://doi.org/10.1186/gb-spotlight-20040427-03; and Andrew Alderson, Richard Gray, and Patrick Hennessy, "Foot and Mouth Lab Failure Causes Outbreak," *Telegraph*, 5 August 2007.