UNIVERSITÄT OSNABRÜCK

Geostrategy and Geopolitics
Department 1
49069 Osnabrueck

Artificial Intelligence in Biological and Chemical Warfare

25 Jan 2023

Summary
Artificial Intelligence (AI) is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing. Overall, the use of AI in life sciences is still in an early stage, but AI tools with relevance for biological and chemical warfare could already be established. This affects the creation of new substances, the identification of potential targets by prediction of protein structures, the detection and identification of suspicious particles and DNA sequences and the defense against malicious actors.
This includes the creation of new compounds related to VX gas by a modified MegaSyn algorithm, and advances in protein structure prediction by AI tools like AlphaFold 2. On the other hand, AI facilitates the detection of suspicious particles (HoloZcan) and DNA sequences (Fun GCAT) and concepts for a holistic biothreat defense (Biothreat Artificial Intelligence Network BAIN) are underway which will be supported by the ongoing development of 6G networks.
An updated overview of biological and chemical weapons will be given. After a brief introduction into the concepts of AI, the relevant AI tools and cyber-biosecurity threats will be presented. The final section will discuss the need for a systematic and coherent oversight regimen.

Content

1 Introduction

Artificial Intelligence (AI) is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing. Overall, the use of AI in life sciences is still in an early stage, but recent advances in AI-based tools in life sciences caused dual-use concerns with respect to development and modification of biological and chemical weapons. These include the creation of new compounds related to VX gas by a modified *MegaSyn* algorithm, and advances in protein structure analysis by AI tools like *AlphaFold 2*. On the other hand, AI facilitates the detection of suspicious particles (*HoloZcan*) and DNA sequences (*Fun GCAT*) and concepts for a holistic biothreat defense (*Biothreat Artificial Intelligence Network BAIN*) are underway which will be supported by the ongoing development of 6G networks[1]. Amongst others, genome and protein engineering including design tools, bioinformatics, predictive modeling, and analytical tools for functional phenotypes are listed as critical and emerging technologies in the United States[2].

2 Biological and Chemical Weapons

2.1 Overview

After the experience with chemical weapons in World War 1, the *1925 Geneva Protocol* prohibited the use of chemical and biological weapons, including poisonous gases, and bacteriological methods of warfare. In 1992, the *Chemical Weapons Convention (CWC)*, more precisely the *Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on Their Destruction* was adopted and became effective in 1997, which forbids the development, stockpiling, or use of any kind of chemical weapons. Under the CWC, the *Organization for the Prohibition of Chemical Weapons (OPCW)* has established a verification and monitoring regime and a network of assistance and protection. The United States and the Soviet Union supported the *United Nations Biological and Toxin Weapons (BTW) Convention* from 1972 which made the development, production and stockpiling of biological and toxin weapons illegal. For biological warfare, no oversight body similar to the OPCW exists[3].

[1] Su et al. 2021
[2] NSTC 2022
[3] Alleslev 2021

From the biochemical perspective, chemical and biological weapons form a kind of continuum with fluid borders and grey zones. This is the reason why in the literature sometimes terms like **biochemical weapons**[4] or 'Bio Chem' or 'BC' occur:

- Pure chemical weapons damage the target by chemical reactions (e.g., chlorine gas which forms hydrochloride HCl which damages tissues by its acidity)
- Some chemical weapons use biochemical (pharmacological) pathways, e.g., toxic nerve agents which block the vital enzyme acetylcholinesterase like *Sarin, VX* or *Novichok*
- A grey area are toxic peptides (bioregulators) where naturally occurring and locally acting hormone-like short amino acid chains such as *Substance P* are vaporized[5]. Substance P is much more toxic than *Sarin*. While in theory such aerosols can provide substantial damage, there are high hurdles in practice. High doses are needed which makes a large-scale vaporization difficult; the resulting production costs are then another high hurdle. As a result, this class of biochemical weapons could not be introduced until today.
- Toxins also target specific biologic pathways and structures to exert their effect, e.g., ricin as protein synthesis blocker. *Ricin* plays a major role as bioterrorist agent. In 2013, a man sent letters containing the herbal toxin ricin to parliamentarians and to President Obama with the expectation that the toxin would be inhaled when the letter is opened. This attempt was detected and failed; the attacker was very quickly identified and imprisoned. A similar attack on President Trump failed in 2018[6]. Based on the surveillance of ricin orders by U.S. authorities, two attempts to build ricin bio-bombs could be stopped in Germany in 2018 and 2022. The explosion heat and pressure of a bomb would likely degrade most or even all toxins or other agents which makes the construction of simple bio-bombs technically very difficult.
- Toxic peptides and toxins are a grey zone, as they fall under the Chemical and Biological Weapons Convention at the same time. *Botulinum toxin, ricin* and *Staphylococcal enterotoxin B (SEB)*, a superantigen with diffuse overstimulation of immune system resulting in a toxic shock have a history as bioweapons, but in nature further natural toxins exist which could be weaponized, in particular[7]:
  - The bacterial *exotoxin STa* secreted by *enterotoxigenic E. coli* binds the guanylate cyclase C receptor, a second messenger element for cellular communication, which disturbs the electrolyte balance. The resulting diarrhea is not lethal.
  - *Gramicidin* produced by the bacterium *B. brevis* form an ionophore (an ion channel) which leads to loss of cellular ions and cell death.
  - *Saxitoxin*, a marine toxin which accumulates in shellfish by algae consumption and blocks nerve cell function by binding to receptor site 1 of voltage-gated sodium channels resulting in paralysis. In total, there is a group of 80,000 marine peptide toxins called *conotoxins*.
  - *Mycotoxins* are metabolic products of fungi. The most relevant group are trichothecenes like T-2 mycotoxin produced by *Fusarium*. They block the protein synthesis by binding to ribosomes. Further mushroom toxins are *amatoxins* that block cells by binding to the cellular RNA polymerase II and *phallotoxins*, which block muscle cells by binding to the muscle protein actin.
- Finally, there are classical biological weapons, i.e., viruses and bacteria as infectious agents. Note that in addition to *Bacillus Anthracis (Anthrax)* some variants of the closely

[4] Sutherland 2008
[5] Kuhn 2004
[6] Saalbach 2019
[7] Lee et al. 2022

related *Bacillus cereus* harbor anthrax-like plasmid genes (pXO1 and pXO2) which cause an anthrax-like disease[8]

In 2022, there was an intense discussion whether genetically modified viruses can constitute a new class of bioweapons. The term *Gain-of-Function (GoF)* describes the gain of new functions by organisms through genetic changes, which can naturally occur or by experimental genetic modifications. Gain-of-Function research on viruses is enhancing transmissibility, virus replication, virulence, host range, immune evasion or drug and vaccine resistance to get insights into the viral mechanisms, to create and analyze animal models, to accelerate drug and vaccine development and to improve pandemic preparedness[9]. Influenza and coronaviruses are main research targets, because they cause pandemics by airborne infections. But the problem with both viruses is that they cannot be targeted or directed as they spread in an uncontrollable manner and could also affect the attacker. This disqualifies genetically modified influenza and corona viruses as bioweapons.

The following table briefly summarizes the current chemical and biological weapons.

[8] Mondange et al. 2022
[9] Saalbach 2022b

Table 1 Overview on Chemical and Biological Weapons

Class	Substances	Mode of Action	Comments
Lung damaging (choking) agents	phosgene (carbonyl chloride, CG), diphosgene (DP), chlorine (CL), Perfluoroisobutene (PFIB) as precursor of fluorophosgene	Irritation and damage of respiratory tract and lungs by formation of HCl and hypochlorous (HOCl) acids	The substance chloropicrin (PS) which was part of this class is now classified as non-lethal irritant
Vesicants (blister agents)	Sulphur mustard (H or distilled HD, Yperite or Lost), nitrogen mustard (HN), arsenical vesicants such as Lewisite (L) and other dichloramines known as "Dicks": ethyldichloroarsine (ED), methyldichloroarsine (MD), and phenyldichloroarsine (PD)	Mustards cause chemical burns (blisters) by alkylation and cross-linking of DNA (cytostatic, mutagenic, and cytotoxic). The trivalent arsenic in lewisite binds to the vital enzyme pyruvate dehydrogenase which affects cellular metabolism.	Nitrogen mustard derivates could be used as anti-cancer treatments. Halogenated oximes, such as phosgene oxime (CX) are urticants causing urticaria
Nerve agents	Organophosphates (G-Series with Sarin [GB], Soman [GD] and Tabun [GA], V-Series [VX and variants] and A series [Novichoks] with A-230, A-232 and A-234) Carbamates	Inhibition of the enzyme Acetylcholin-Esterase (AChE) resulting in a life-threating malfunction of nerves and muscles up to paralysis, convulsions and finally death	Some carbamates can be medically used against Alzheimer's disease by brain stimulation. Organophosphorus compounds are widely used as insecticides
Blood agents (cyanide compounds)	hydrogen cyanide (HCN) and cyanogen chloride (CNCl) arsine (arsenic trihydride, AsH3) gas	block the blood oxygen transporter hemoglobin by formation of so-called methemoglobin	An antidote is hydroxycobalamine (Vitamin B12)
Toxic peptides (bioregulators)	Substance P Neurokinin A	Massive stimulation of nerve system	A theoretical new class of weapons
Toxins	Botulinum toxin in the spores of the bacillus *Clostridium botulinum*	Causes a life-threatening neuromuscular paralysis, known as botulism	Low-dose botulinum toxin injections are used as medical treatment of neuromuscular spasms and as cosmetics (face relaxation)
	Ricin, a protein in the castor oil plant Ricinus communis	Blocks protein synthesis until cell death	In South America, the related substance abrin exists
	Staphylococcal enterotoxin B (SEB)	SEB is a superantigen with diffuse overstimulation of immune system resulting in a toxic shock	
Viruses	Smallpox (*Variola major*)	oral infection, a massive viral replication takes place, then it returns to body surfaces (mucosa and skin with multiple lesions) allowing infection of others	
	Viral hemorrhagic fevers (VHF) including *Ebola Virus, Marburg Virus* and others	Cause severe inner bleedings (e.g., as spontaneous nose bleeding).	
Bacteria	Anthrax (*Bacillus anthracis*) can form inhalable spores which contact immune cells. Some *Bacillus cereus* variants can cause an anthrax-like disease	Certain anthrax proteins cause hyperinflammation, an overactive immune system with shock-like symptoms.	Vaccination and antibiotics such as ciprofloxacin as countermeasures
	Francisella tularensis	Tularaemia is a highly infectious disease leading to severe fever and sepsis symptoms.	Antibiotics such as streptomycin and gentamicin as countermeasures
	Yersinia pestis	Yersinia pestis causes plague, typically transmitted by infected flea with painful lymph node swelling (buboes), then sepsis as Black Death.	The antibiotic streptomycin as countermeasure
Bacteria	*Coxiella burnetii* (a bacteria-like organism)	Causes Q-fever that may lead to pneumonia (lung infection), but also to chronic heart valve infections.	Antibiotics of tetracycline type, gyrase blockers are used

Source: Sutherland 2008, OPCW 2019, Stefanopoulos et al. 2022, Mondange et al. 2022, Saalbach 2019 and 2022a

2.2 Other Weapons

There are various **non-lethal chemical weapons (NLWs)** which are commonly grouped as:

- **Riot control agents (RCAs)** that induce skin and eye irritation and inflammation of the upper respiratory system such as *chloroacetophenone (CN), chlorobenzylidenemalononitrile (CS)* and *dibenzoxazepine (CR)*. CS gas is widely used. *Diphenylaminearsine (Adamsit, Clark I)* was considered as mucous irritant and **vomiting agent**. **Malodorants** that produce e.g., a strong skatolic (faecal) odor were also considered and tested as RCAs. A widely used agent is **pepper spray** containing *oleoresin capsicum*, an oily extract of pepper plants of the genus capsicum. The key substance of pepper spray is *capsaicin (trans-8-methyl-Nvanillyl-6-nonenamide)*.
- **Incapacitating agents** have a stronger effect. Hallucinatory *D-lysergic acid diethylamide (LSD)* gas and the acetylcholine-blocking *3-Quinuclidinyl benzylate (BZ)* were tested as **psychedelic warfare**[10] agents, but their effect was not predictable enough. Also, there was a risk of downwind contamination.
- Psychoactive **calmatives** such benzodiazepines and substances that affect neurologically important receptors for adrenaline, dopamine, serotonin, opioids, corticotropin etc. were tested since the 1990ies but not yet introduced. An exception is the use of the strong morphine derivate *fentanyl* which is an important pain medication and also used during anesthesia for surgery. A gas containing fentanyl derivates (mixture of *carfentanil* and *remifentanil*, both more than 1,000 times stronger than methadone) was used against 50 Chechen terrorists who took approximately 800 hostages in the *Dubrovka Theatrical Centre* in Moscow in 2002[11]. The idea was that all persons would fall asleep which happened, but at least 125 hostages died showing the dangers of strong opioid gas[12].

As AI-based tools are increasingly used for drug development as well, the NLWs may also be affected by the progress of this technology. In addition to lethal and non-lethal chemical weapons, there is a third group, the **traditional agents** with arrow poisons such as *curare* (*tubocurarine*, a muscle relaxant) and the Strophantin-related cardioglykoside *ouabain*[13].

[10] Sutherland 2008
[11] Pitschmann/Hon 2023
[12] Sutherland 2008
[13] Pitschmann/Hon 2023

3 Artificial Intelligence

3.1 Definitions and Approaches

Artificial Intelligence (AI) is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing.

Even for human intelligence, there is no standard definition. However, the core of human intelligence definitions includes the mental capacity to recognize, analyze and solve problems, and a human being is then more intelligent if this can be done faster and/or for more complex problems. Based on this, the *United States Department of Defense (DoD)* introduced a working definition that defines AI as: "ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action— whether digitally or as the smart software behind autonomous physical systems"[14].

Many definitions focus on activities that require human intelligence, but strictly spoken, already the simple pocket calculators of the 1970ies made something that normally requires human intelligence. However, it is evident from literature, the AI researchers mean advanced and autonomous computing when they talk about AI.

The leading AI applications are:

- **Deep learning/machine learning** (utilizing memory data for iterative improvement)
- **Neural networks** (layers or nodes for input processing and pattern recognition)
- **Natural Language Processing** (algorithms to understand human language by systematic analysis of the language elements and their relations).
- **Edge computing** (intermediate servers for clouds) and
- **Robotics** including supportive machines (co-bots).

For the AI tools presented in this paper, **machine learning** is the most important application. For machine learning, data from data bases are utilized by the algorithms of the AI to calculate a result. This result can be compared with target parameters and then the next round of calculation starts. The repeat cycles which use the results of the previous cycles are called iterative process.

Another emerging area is **Natural Language Processing (NLP)**. Both the genetic code as well as amino acids are coded with standardized letters in literature[15]. NLP applications do not only read the text, but the algorithms are used to analyze the structure and rules[16]. The convergence of linguistics and biological codes forms the new area of **biolinguistics**.

But this means that the precision of AI tools is not only dependent from the quality of the computer program, but also from the amount of data that can be used for learning. The rapid advance of machine learning is also caused by the rapid growth of chemical, pharmaceutical, genomic and protein databases. As a result, AI can e.g., be used effectively in different parts of drug discovery, including drug design, chemical synthesis, drug screening, poly-pharmacology (multi-target drugs), and drug repurposing[17].

Since 2020, substantial investments were made to fund companies applying AI in drug discovery and also to create cooperations between pharmaceutical companies and companies with a focus on applying AI in drug discovery, e.g., the firm *Exscientia* with its AI drug discovery platform *Centaur Chemist* has established cooperations with *Bristol Myers Squibb*

[14] DoD 2018
[15] Enguix/Jiménez-López 2012, Ofer 2021
[16] Enguix/Jiménez-López 2012
[17] Paul et al. 2021

(BMS), Sanofi, Bayer, GlaxoSmithKline, Roche, Rallybio and the *University of Oxford*, while *Microsoft* partners with *Novartis* and so on[18].

On the other hand, AI in this area is still in an early stage and there is a substantial difference between AI output in ideal experimental settings and the real-world practice[19]. Currently, AI applications still have a limited role[20].

Nevertheless, AI tools with relevance for biological and chemical warfare could already be established. This affects the creation of new substances, the identification of potential targets by prediction of protein structures, the detection and identification of suspicious particles and DNA sequences and the defense against malicious actors.

This includes the creation of new compounds related to VX gas by a modified *MegaSyn* algorithm, and advances in protein structure prediction by AI tools like *AlphaFold 2*. On the other hand, AI facilitates the detection of suspicious particles (*HoloZcan*) and DNA sequences (*Fun GCAT*) and concepts for a holistic biothreat defense (*Biothreat Artificial Intelligence Network BAIN*) are underway which will be supported by the ongoing development of 6G networks.

3.2 AI-based Tools

3.2.1 Modified MegaSyn Algorithm

MegaSyn is an AI-based drug discovery program which is based on machine learning to get *de novo* molecules. It is only one of various commercial programs in this area, but was subject of a major chemical warfare experiment by Urbina et al[21]. In its regular setting, *MegaSyn* rewards bioactivity, but avoids toxicity to gain effective, but safe new molecules that could be used as potential new drug candidates.

But if the logic is inverted and bioactivity and toxicity are both rewarded, the program generates new toxins. As this approach is too unspecific, the AI was trained for neurological disorders and its treatments. Then, VX gas was set as target molecule which is a strong anticholinergic substance (some anticholinergics are also used as medication to treat the neurological disorder Alzheimer's disease). As a result, the modified *MegaSyn* algorithm created in only 6 hours over 40,000 new molecules with chemical weapon potential, some even more toxic than VX[22].

Details of the training procedure were not published for security reasons, but the message is clear: modified AI-based drug research tools which are directed against a vital target (enzyme, protein) are able to create toxic agents with chemical weapon potential. This is the reason why the increased ability of AI-tools to analyze target proteins as shown in the next section may facilitate malicious activities as well.

However, there are some limitations. A molecule created by a computer is not automatically a new chemical weapon. The molecules need to be evaluated and tested whether they really meet the selection criteria of the algorithm. The chemical properties are another hurdle. The molecules need to be easily synthesized with reasonable costs, they need to be stable at room temperature and they need to be vaporized. Ideally, they also need to penetrate protective clothing.

Probably the most created molecules will not meet all of these criteria, but as there were thousands of new compounds, it is likely that some of them meet these criteria and have a new molecular structure. This is a major problem, because the CWC forbids all chemical weapons,

[18] Salvage 2021
[19] Pesheva 2022
[20] Brockmann et al. 2019
[21] Urbina et al. 2022
[22] Urbina et al. 2022

but in practice, the focus of the OPCW is on the molecules listed in *CWC Verification Annex* with three schedules of chemicals with a particular risk level. The schedules form the basis of the mandatory declarations and routine industry inspections by the OPCW. Schedule 1 includes chemicals and toxins, which have been developed, produced, stockpiled, or used as chemical weapons[23]. A new molecular structure which is not known as chemical weapon will likely slip through the OPCW oversight and could be produced without suspicion.

For this reason, it would make sense if the OPCW and Intelligence Communities repeat the experiment of Urbina et al. for VX and other known chemical weapons. The created AI-based molecules with chemical weapon potential could be listed on a non-public 'shadow list'. In case that inspections or investigations find chemicals, an automated comparison against this list would quickly clarify a potential chemical weapon attempt. As it can be expected that malicious actors also try to find something with modified AI algorithms, this shadow list is strongly recommended and urgent. For biological weapons, the *Fun GCAT* and *BAIN* tools presented below are developed to cover this matter.

In addition to molecules, AI can also facilitate the search for antibodies that fit to a certain target. During the COVID-19 crisis, the *U.S. Department of Energy (DOE)* established the *National Virtual Biotechnology Laboratory (NVBL)* in March 2022. The NVBL used AI methods to computationally screen 10^{40} possible antibody variations, identifying the best hits that could be used as an antiviral against the *Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2)* spike protein[24].

There are no regulations for a safe technical design of drug discovery tools.

3.2.2 AlphaFold 2 and RoseTTAFold

The AI-based programs *AlphaFold 2* and *RoseTTAFold* are designed for protein structure prediction and analysis in general and not intended for dual use or biological and chemical warfare. However, the already created findings of *AlphaFold* (meanwhile as advanced *AlphaFold 2*) since its introduction resulted in an exponential growth of precisely clarified protein structures which means an exponential growth of potential targets for biological and chemical weapons as well, because the exact structure of a target is a pre-requisite to design new molecules. As a consequence, *AlphaFold 2* and *RoseTTAFold* are planned to be integrated in the upcoming concept of a *Biosecurity Artificial Intelligence Network (BAIN)*[25] which will be described later on.

DeepMind's AlphaFold 2 was the first AI-based approach capable of predicting protein structures to near experimental accuracy in a majority of cases[26]. Protein prediction methods are usually tested against proteins that are presented at the bi-annual *Critical Assessment of protein Structure Prediction (CASP)* meeting and that have not been deposited in the *protein database (PDB)* and were not publicly disclosed, i.e., they could be used as a real test. *AlphaFold* was originally developed based on the CASP13 meeting data, but *AlphaFold 2* is a completely different machine-learning model and based on the CASP14 assessment (May–July 2020)[27]. The *AlphaFold* network directly predicts the three-dimensional (3D) coordinates of all heavy atoms for a given protein using the primary amino acid sequence and aligned sequences of homologues as inputs and processes them in a *graphics processing unit (GPU)*.[28]

[23] OPCW 2021
[24] NVBL 2021
[25] Lee et al. 2022
[26] Jumper 2021
[27] Jumper 2021
[28] Jumper et al. 2021

For the three-dimensional prediction (1D = sequence level, 2D = distance, 3D = coordinates), reasoning about 3D atomic coordinates in the two-track *AlphaFold2* architecture happens after processing of the 1D and 2D information is complete[29].

Meanwhile, *RoseTTAFold* was developed as alternative with a three-track network in which information at the 1D sequence level, the 2D distance map level, and the 3D coordinate level is successively transformed and integrated by a permanent flow of information between all three levels[30].

3.2.3 HoloZcan

The *European Union* was funding the *HoloZcan* project within the *Horizon 2020* research program to develop a field-deployable rapid multiple biosensing system for detection of chemical and biological warfare agents. *HoloZcan* is a combination of optical and digital holographic detection methods with mature machine learning and artificial intelligence software to solve the problem of rapid response time and connectivity with other existing sub-systems[31].

Theoretically, *HoloZcan* can detect particles from 50 micrometers (µm) on, but practically above 0.250 µm particle range, the phase and intensity plane characteristic were optimal to improve detection performance, which makes object detection and classification possible within the dimensional range of bacteria[32].

3.2.4 Fun GCAT

The automatization of desoxyribonucleic acids (DNA) has made substantial progress and it should be noted that in 2020 the full-length genome sequences of 9,240 different viruses, including the smallpox virus, were publicly available in an online database maintained by the *U.S. National Institutes of Health (NIH)*[33] which has a potential for misuse[34]. Meanwhile, synthesized DNA can be commercially ordered. Together with database information extinct viruses can be recreated as synthetic virus solely on database information and commercially ordered synthetic DNA. The extinct *horsepox virus* could be synthesized, but also fully synthetic vaccinia viruses, one of the largest naturally existing viruses[35]. Synthetic DNA can be used for creation of harmful pathogens which requires a surveillance of this production.

The *Intelligence Advanced Research Projects Activity (IARPA)* is developing the *Functional Genomic and Computational Assessment of Threats (Fun GCAT)*[36]. *Fun GCAT* is the computational analysis of DNA and answers three questions per sequence: What organism does it come from? What biological functions does it have? How dangerous is it? Neural networks and other bioinformatic tools are used to learn the common patterns of sequences with similar origins and functions, resulting in a 500 times higher computational efficiency over state-of-the-art and stable performance also for short (<50 base pairs) sequences. The U.S. Intelligence Community can now conduct relevant missions from rapid screening of very large datasets to field-based, targeted analysis[37]. A practical application could be the *Biological Defense Threat Reduction Program (BTRP)* by the *U.S. Defense Threat Reduction Agency (DTRA)* which

[29] Baek et al. 2021
[30] Baek et al. 2021
[31] Palhalmi et al. 2022
[32] Palhalmi et al. 2022
[33] Wikipedia entry for Synthetic Virology 20 Nov 2022
[34] Smith/Sandbrink 2022
[35] Noyce et al. 2018
[36] IARPA 2022
[37] IARPA 2022

supports biosafety labs in Asia and Africa, but e.g., also the Ukraine to implement and maintain high biosafety and biosecurity standards[38].

An ongoing problem which also applicable for civilian version BAIN (next section) is a lack of a mandatory regulation.

The revised *2022 United States Department of Health and Human Services (HHS) Screening Framework Guidance for Providers and Users of Synthetic Oligonucleotides (Proposed Revised Guidance)* will cover providers and customers of synthetic DNA and RNA[39]. The guidance recommends that providers perform customer and sequence screening and in case of concerns, providers should perform a follow-up screening where authorities may be asked for advice, like the *FBI Field Office Weapons of Mass Destruction (WMD) Coordinator*. The guidance particular addresses sequence of concerns (SOC). For SOCs, documents should be retained for at least 8 years. Manufacturers should provide a data logging function to maintain a record of the synthesized sequences. The order batch size should be considered as well to identify orders of small oligonucleotides that could be assembled into larger sequences of concern[40]. A transfer to any other individuals should be documented as well

The revised guidance will still be voluntary. The approach is "know your client"[41], i.e., to be aware of uncommon orders from persons or institutions without legitimate needs. A part of this strategy are provider and scientific organizations that engage their members to adhere to high standards. While large synthesis companies alert each other in case of problems, this does not cover smaller and foreign companies. This means that there are **substantial oversight gaps**.

A low-cost solution could be a database held by public authorities which collects all information about individual or organizations with known inappropriate handling, misuse or requests that were not legitimate (similar to the *U.S. Food and Drug Administration FDA* database which listed investigators with issues in clinical studies). The only requirement would be that problematic clients or requests are reported to this database, i.e. it would not be necessary to disclose all clients (which could be business confidential). This would allow even small companies as well as foreign companies a quick background check whether an individual or organization is already known for biosecurity issues.

Another issue are **commercial virus production services**. Meanwhile, it is not necessary anymore to request DNA sequences as complete viruses can be ordered as well, e.g., adenoviruses, but also genetically engineered vaccinia viruses. This is combined with other services like 24 h-service or fast shipping which shows how low the technical hurdles meanwhile are. The guidance should explicitly mention the order of full viruses as well.

3.2.5 Biosecurity Artificial Intelligence Network (BAIN)

The *Biosecurity Artificial Intelligence Network (BAIN)* is an AI-based concept that will be similar to Fun GCAT[42] and will conduct a holistic biosecurity surveillance by combination of the following elements:

- Screening of every commercial nucleic acid order (including gene blocks and oligonucleotides) and peptide order against a database containing genomic and proteomic data of known pathogens as well as toxic peptides and proteins.
- Based on machine learning, programs for *in silico* bioactivity prediction will allow identification of potentially toxic or dangerous gene products.

[38] DTRA 2020
[39] HHS 2010, 2022
[40] HHS 2022
[41] Nature 2021
[42] Lee et al. 2022

- BAIN will also integrate existing programs such as *RoseTTAFold* and DeepMind's *AlphaFold2*[43].
- The AI capabilities of BAIN allow to compile customer profiles, orders, screening results, and build a user network that also categorizes each user's research areas using user-submitted data and web scraping. This would allow to detect both abnormal behavior of individuals and institutions.

While BAIN could be implemented already now from a technical standpoint, there are legal and practical obstacles. The US guidance is voluntary and lacks legal enforcement. Voluntary participation is possible, but the above-described issues (disclosure of clients, business confidentiality, smaller and foreign actors may not join or cooperate) undermine the BAIN concept. Again, the full virus production is not explicitly covered. For this reason, a public blacklist of individuals or institutions with biosafety and biosecurity issues maybe an easier solution which would require only the legal obligation to report security issues with clients.

3.2.6 6G Networks

Meanwhile, 5G networks are globally established, but the research is already heading towards 6G. The advantages of **6G networks** will be high data transmission speed (up to 1 terabyte per second), wireless hyper-connectivity (100 million connections per km^2), low end-to-end latency (< 1 ms), reliability and high-accuracy positioning capabilities (indoor: <10 cm in 3D; outdoor: <1 m in 3D)[44]. Once established, 6G-based AI technologies can be used to address issues ranging from early detection of bio-disasters to public health interventions and disaster recovery. Analysis of social media may contribute to rapid responses by detection of abnormalities (e.g., increased reporting of certain symptoms or occurrence of abnormal behaviors).

4 Cyber-biosecurity

Cyber-biosecurity aims to identify and mitigate security risks by digitalization and automation of biotechnology[45].

In principle, computer systems in research units are confronted with the same cyber threats than all other computers. In particular, hospitals, universities and research units are increasingly confronted with ransomware attacks with blocking and stealing of health and research data. In his paper, Cebo identifies seven prominent cyber-biosecurity attack types: sabotaging, corporate espionage, spam emails, data breaches, distributed denial of service (DDoS) attacks, password threats, and criminal attacks[46].

As AI in biotechnology heavily relies on data sets and data bases, the manipulation of data and the **data poisoning** by mislabeled data can mislead AI-driven technologies with corrupting or destroying industrial bio-intelligence[47]. **Data theft** can affect biosecurity if information about harmful agents is stolen, may target research secrets (patents), but can also affect individuals be stealing their health and genetic information[48].

The growing amount of genetic data raised the question whether a **super-targeted biological warfare** would be possible where certain groups of people (e.g., ethnic groups) who have a specific genetic variant in common or even individuals could be attacked with a tailor-made

[43] Su et al. 2021
[44] Su et al. 2021
[45] ENISA 2022
[46] Cebo 2022
[47] Pauwels 2019, 2021
[48] Cebo 2022

biological weapon. This concept was already discussed in previous decades as so-called **ethnic bomb**.

The point is that not every gene produces something that can be approached by a toxin or bioweapon. Many variants are minimal, which makes a selective attack impossible. So far, no variation could be weaponized. Medically relevant genetic differences between ethnics exist (e.g., tolerance against paracetamol/acetaminophen), but no genetic variance allowing a bio-attack on a certain population is known yet, that is, a super-targeted biological warfare or ethnic bomb remains hypothetical.

Manipulated devices or processes available can lead to misdetection attacks where the device or service could appear to be functioning while it actually provides false results[49].

A new research area evaluates synthetic DNA as a relatively stable storage medium. The DNA is then produced by synthesis and assembly and later on analyzed and decoded by sequencers. Many DNA sequencing systems code the nucleotides adenine, thymine, cytosine, and guanine (A, T, C, and G) of the DNA as bit combination - A is coded as 00, C as 01, G as 10, and T as 11. Even hundreds of Gigabytes result in a DNA piece that looks like a very small and thin piece of a hair. This allows covert data transportation in a practically invisible and undetectable manner. Researchers from *Harvard University* were able to insert coded DNA into an *Escherichia coli* bacterium[50].

Researchers of the *University of Washington* were encoding computer malware into a DNA segment. When this part of the DNA ran through a sequencer with an analysis program, the code infected the computer and the attackers were able to get control over the attached computer. The experiment was quite complicated, but it showed that it is possible to intrude companies that work with DNA by sending maliciously encoded DNA[51].

5 Discussion and Conclusion

Artificial Intelligence tools are mostly still in an early stage and there is a substantial difference between AI output in ideal experimental settings and the real-world practice. Currently, AI applications still have a limited role. Nevertheless, AI tools with relevance for biological and chemical warfare could already be established. This affects the creation of new substances, the identification of potential targets by prediction of protein structures, the detection and identification of suspicious particles and DNA sequences and the defense against malicious actors.

The creation of harmful agents by manipulated AI drug discovery tools is meanwhile possible and it was apparent that only simple modifications of the algorithm in combination with chosen target molecules are sufficient to gain new chemical weapons. The rise of protein structure prediction by AI-based tools like *AlphaFold2* leads to a rapid increase of precisely defined potential targets for a biological or chemical attack.

A major problem of the chemical weapon regulation is the focus of the OPCW on molecules listed in *CWC Verification Annex*, while new molecules which are not known as chemical weapon will likely slip through the OPCW oversight and could be produced without suspicion.

For this reason, it is recommended that OPCW and Intelligence Communities repeat the experiment of Urbina et al. for VX and other known chemical weapons to get a non-public ‘shadow list’ of AI-based molecules with chemical weapon potential to allow automated comparison against this list. As it can be expected that malicious actors also try to find

[49] ENISA 2022
[50] NATO 2021
[51] Ney et al. 2017

something with modified AI algorithms, this step is urgent. There are no regulations for a safe technical design of drug discovery tools.

For biological weapons, the *Fun GCAT* and *BAIN* tools are developed to ensure biosecurity, but there are legal and technical matters.

The revised guidance for DNA and RNA synthesis in the U.S. will still be voluntary. While large synthesis companies alert each other in case of problems, this does not cover smaller and foreign companies. Furthermore, commercial virus production services are not explicitly covered. This means that there are substantial oversight gaps.

A low-cost solution could be a database held by public authorities which collects all information about individual or organizations with known inappropriate handling, misuse or requests that were not legitimate. The only legal requirement would be that problematic clients or requests are reported to this database, i.e., it would not be necessary to disclose all clients (which could be business confidential). This would allow even small companies as well as foreign companies a quick background check whether an individual or organization is already known for biosecurity issues. The guidance should explicitly mention the order of full viruses as well. In conclusion, AI-based tools are already relevant for chemical and biological warfare, both for threats and for defense and there is need for a more systematic regulation.

6 References

Alleslev, L. (2021): Biological Weapons: Technological Progress and the Specter of Bioterrorism in the Post-Covid-19 Era. Science and Technology Committee (STC) of the NATO Parliamentary Assembly - Sub-Committee on Technological Trends and Security (STCTTS). Preliminary Draft Report 024 STCTTS 21 E 22 March 2021

Baek, M. et al. (2021): Accurate prediction of protein structures and interactions using a three-track neural network. Science 10.1126/science.abj8754 (2021).

Brockmann, K. et al. (2019): BIO PLUS X. Arms Control and the Convergence of Biology and Emerging Technologies. SIPRI Paper March 2019

Cebo, D. (2022): Strategical Analysis of Cyberbiosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.20485929.v1

DoD (2018): U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.

DTRA (2020): The official eBook of DTRA-JSTO. Defense Threat Reduction Agency (DTRA)-Joint Science and Technology Office (JSTO), Federal Select Agent Program. Annual report of the federal select agent program.

Enguix, G.B., Jiménez-López, M.D. (2012): Natural Language and The Genetic Code: From The Semiotic Analogy. To Biolinguistics. Proceedings of the 10th World Congress of the International Association for Semiotic Studies (IASS/AIS). Universidade da Coruña (España / Spain), 2012. ISBN: 978-84-9749-522-6 Pp. 771-780

ENISA (2022): Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation. Needs and Priorities of the European Union Agency for Cybersecurity ENISA. May 2022

HHS (2010): United States Department of Health and Human Services (HHS) Screening Framework Guidance for Providers of Synthetic Oligonucleotides. Final Guidance

HHS (2022): United States Department of Health and Human Services (HHS) Screening Framework Guidance for Providers and Users of Synthetic Oligonucleotides, Summary of Updates in Response to Public Comments Received in 2020

Jumper, J. et al. (2021): Highly accurate protein structure prediction with AlphaFold. Nature Vol 596, 26 August 2021:583-589 https://doi.org/10.1038/s41586-021-03819-2

Kuhn, J. (2004): Biologische Waffen. In: Mietzsch, A. (Ed.): Kursbuch Biopolitik. Biocom AG Verlag 2004 p.147-161

Lee, Y-CJ., Cowan, A. and Tankard, A. (2022): Peptide Toxins as Biothreats and the Potential for AI Systems to Enhance Biosecurity. Front. Bioeng. Biotechnol. 10:860390. doi: 10.3389/fbioe.2022.860390

Mondange, L., Tessier, É., Tournier, J.-N. (2022): Pathogenic Bacilli as an Emerging Biothreat? Pathogens 2022, 11, 1186. https://doi.org/10.3390/pathogens11101186

NATO (2021): Emerging Threats of Synthetic Biology and Biotechnology. Edited by Trump, B.D., Florin, M.V., Perkins, E. and Linkov, I. Proceedings of the NATO Advanced Research Workshop on Security and Resilience Addressing Emerging Synthetic Biology and Biotechnology Threats Lausanne, Switzerland

Nature (2021): Synthetic virology: the experts speak. Nature Biotechnology, Vol. 39, October 2021, pp. 1185–1193

Ney, P. et al. (2017): Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More. Proceedings of the 26th USENIX Security Symposium August 16–18, 2017 Vancouver, BC, Canada ISBN 978-1-931971-40-9

Noyce, R.S. et al. (2018): Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. PLoS One 13, e0188453. https://doi.org/10.1371/journal.pone.0188453

NTSC (2022): Critical and emerging technologies list update. A Report by the Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council (NTSC). February 2022

NVBL (2021): U.S. Department of Energy - R&D for Rapid Response to the COVID-19 Crisis - National Virtual Biotechnology Laboratory Brochure January 2021

Ofer, D., Brandes, N., Linia, M. (2021): The language of proteins: NLP, machine learning & protein sequences. Computational and Structural Biotechnology Journal 19 (2021) 1750–1758

OPCW (2019): International Cooperation and Assistance Division Assistance and Protection Branch. Practical Guide for Medical Management of Chemical Warfare Casualties of the Organization for the Prohibition of Chemical Weapons OPCW.

OPCW (2021): Annex on Chemicals Schedule 1 of the Chemical Weapons Convention. Organization for the Prohibition of Chemical Weapons. Available from https://www.opcw.org/chemicalweapons-convention/annexes/annex-chemicals/schedule-1

Palhalmi, J. et al. (2022): Theoretical limits and perspectives of the digital holographic technology in bio-detection related on-field decision making. CBRNE Innovation Conference Lille 2022

Paul, D. et al. (2021): Artificial intelligence in drug discovery and development. Drug Discovery Today Volume 26, Number 1 January 2021 https://doi.org/10.1016/j.drudis.2020.10.010

Pauwels, E. (2019): The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI, United Nations University Centre for Policy Research, 29 April 2019.

Pauwels, E. (2021): Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Hybrid CoE Strategic Analysis / 26 May 2021

Pesheva, E. (2021): Can AI transform way we discover new drugs? Harvard News 17 November 2022 https://hms.harvard.edu/news/can-ai-transform-way-we-discover-new-drugs

Pitschmann, V., Hon, Z. (2023): Drugs as Chemical Weapons: Past and Perspectives. Toxics 2023, 11, 52. https://doi.org/10.3390/toxics11010052

Saalbach, K. (2019): Biological Warfare – in Schmidt, T. (Ed.): Encyclopedia of Microbiology (Fourth Edition), pages 520-525 Academic Press Elsevier ISBN: 9780128117361 https://doi.org/10.1016/B978-0-12-801238-3.62160-8

Saalbach, K. (2022a): Therapeutic Treatment of Nerve Agent Toxicity. Chapter 24 in: Das, S., Thomas, S., Pratim, P. (Editors) Sensing of Deadly Toxic Chemical Warfare Agents, Nerve Agent Simulants, and their Toxicological Aspects, pages 569-585. 1st Edition 23rd September 2022- Elsevier ISBN: 978-0-323-90553-4 https://doi.org/10.1016/B978-0-323-90553-4.00019-6

Saalbach, K. (2022b): Gain-of-Function Research. Chapter 3 in: Gadd/Sariaslani (Editors) Advances in Applied Microbiology, Edition 120, 12 October 2022, pp. 79-111. William Andrew Publishing. ISBN 978-0-323-98969-5 https://doi.org/10.1016/bs.aambs.2022.06.002

Salvage, N. (2021): Tapping into the drug discovery potential of AI. www.nature.com/biopharmdeal June 2021, p.B37-B39

Smith J.A., Sandbrink J.B. (2022): Biosecurity in an age of open science. PLoS Biol 20(4): e3001600. https://doi.org/10.1371/journal.pbio.3001600

Stefanopoulos, P., Aloizos, S., Tsironi, M. (2022): Clinical symptoms of chemical warfare agents toxicity including mustards, halogenated oximes, arsenicals, and toxins poisoning. Chapter 19 in: Das, S., Thomas, S., Pratim, P. (Editors) Sensing of Deadly Toxic Chemical Warfare Agents, Nerve Agent Simulants, and their Toxicological Aspects, pages 431-472. 1st Edition 23rd September 2022- Elsevier ISBN: 978-0-323-90553-4

Su, Z. et al. (2021): Addressing Biodisaster X Threats With Artificial Intelligence and 6G Technologies: Literature Review and Critical Insights J Med Internet Res 2021;23(5):e26109 doi: 10.2196/26109

Sutherland, R.G. (2008): Chemical and Biochemical Non-lethal Weapons. Political and Technical Aspects. SIPRI Policy Paper No. 23

Tonix (2020): Tonix Pharmaceuticals Presented Results from a Preclinical Study of TNX-801, a Potential Vaccine to Prevent Smallpox and Monkeypox, in a Poster Presentation at the 2020 American Society for Microbiology (ASM) Biothreats Conference. New York, 29 Jan 2020

Urbina, F. et al. (2022): Dual use of artificial-intelligence-powered drug discovery. Nature Machine Intelligence, Vol 4 March 2022, 189-191