Dany Shoham[1]

Chemical and Biological Weapons

Given the variability in defining hybrid warfare, perhaps the most simple and decent form would rely on the definition of 'hybrid', namely, "something that is a mixture of two very different things" (Cambridge Dictionary), meaning that hybrid warfare is plainly a mixture of two (or more) very different warfares. The pertinent scope is broad. Alongside conventional warfare, unconventional warfare is one main vector within this context, and includes, i.a. chemical and biological weapons (CBW). In similarity to radiological weapons, and unlike nuclear weapons, CBW constitute weaponry of mass destruction having no physical impact. CBW may expectedly be used in parallel to any other type of warfare, particularly together with information warfare aiming to deny or, conversely, take responsibility and advantage of, or just threaten their employment; otherwise, as another example, together with cyber warfare aiming to paralyse hospitals or pharmaceutical producers, and thus hinder medical treatment and preventive measures. Many parameters account for remarkable flexibility in employing CBW, thereby shaping a wide range of tasks/tentative achievements, as well as adjustability, in relation to the contemporarily employed other type(s) of warfare, being it conventional or an additional type of unconventional warfare. Especially notable among those parameters – together with actual instances – are:

- the user – a state (Syria, during the civil war) or non-state actors – an organisation (ISIS, in Iraq and in Syria)
- the contemporaneously conducted warfare – during the civil war in Syria, CW were often used by Syria parallel to conventional warfare; at times lethal (sarin nerve agent) and at times non-lethal (chlorine, basically an incapacitant); also, nearby hospitals were attacked at the same time, so as to hamper treatment and/or obfuscate evidence
- the impact – intended to form, and thereafter last, in the short, medium, or long run; for example, the impact of a non-persistent nerve agent, as compared to an epidemic virus (having a period of incubation, and prolonged effect)

[1] Bar-Ilan University.

DOI: https://doi.org/10.36250/01236_05

- the objective – the direct impact may be the ultimate objective, or may propel the occurrence of the ultimate objective; the CW employment in Syria was meant, alternately, to afflict and/or terrorise Syrian citizens and ISIS warriors
- the target – humans, livestock or crops; also, logistic targets, such as fuel pools, can be contaminated by fuel-eating germs, as one instance
- the mode – through commando operations (assassinations with toxic substances by Russia and North Korea) or through standardised munitions (Iraq, Syria)

On the whole, CBW are highly consistent with the increasing global trend of combining conventional and unconventional warfares. A substantial spectrum of hybrid warfare modes is thereby accentuated, at large, serving for the attainment of noticeably diversified outcomes. The main problem marking the menace described here, hence, is the complicatedness of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers. This problem is intended to be handled through typologically and detailedly expounding this coupling, so as to enhance preparedness and countering capacities. At its basic level, hybrid warfare represents the coupling of conventional and unconventional warfares, while chemical and biological weapons (CBW) are included within the unconventional vector. At its utmost, namely under the category termed 'Unrestricted Hybrid Warfare' – foremost conceptualised and upgraded by China and Russia – there are three sub-categories: non-military, transitional and military. Both approaches are being followed in the present chapter, within a spectrum of CBW events and scenarios. The chemical and biological warfare agents (CBA) and weapons mentioned in this chapter are not all prohibited under the CB conventions. The purpose of mentioning the CBW discussed here is to broadly present a variety of such agents and weapons that might be effectively employed within the context of hybrid warfare, whether or not included in those conventions. Alongside classic CBW, the nearly existing horizon of hybrid warfare is apt to combine conventional warfare modes together with new generations of a variety of CBW, as detailed below. A variant of hybrid warfare can include two vectors (or more), of which one is a CBW vector, and the second one (either an additional CBW or a conventional element) serves to prevent attention to, detection and identification (by the opponent) of the first one; or brings about a synergistic effect together with the first one. An example is simultaneous employment of CW munitions together with conventional munitions that

look entirely the same. Or simultaneous employment of CW munitions containing one type of a CWA together with another type of CWA-containing munitions that look entirely the same. The element of misleading is hence prominent, alongside. In sum, this chapter is intended to meet pertinent questions and issues as follows:

- the singularities of CBW as weapons of mass destruction
- the meaningfulness of CBW as a vector within the doctrine of hybrid warfare at large
- within that context – the consequentiality of the category termed 'Unrestricted Hybrid Warfare', foremost conceptualised and upgraded by China and Russia
- the actuality of events and feasible scenarios, which expound the complicatedness and impacts of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers
- typologically and detailedly expounding this coupling, so as to enhance preparedness and countering capacities
- the utilities of CBW in hybrid warfare beyond anti-human effects, namely for attacking farm animals, crops, wild vegetation (defoliants), and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare
- the weight of a nearly existing horizon of hybrid warfare apt to combine conventional warfare modes together with new generations of a variety of by far advanced CBW

Delivery and dispersion

Operationally, the effectiveness of CBW is mainly shaped by the efficiency of its delivery, or dissemination, to a target. The most common techniques include munitions (such as bombs, projectiles, warheads) that allow dissemination at a distance and spray tanks which disseminate from low-flying aircraft. Developments in the techniques of filling and storage of munitions have also been important in shaping the effectiveness of CBW. The dissemination is highly dependent on atmospheric conditions because many CWAs act in gaseous form. Thus, weather observations and forecasting are essential to optimise weapon delivery and reduce the risk of injuring friendly forces. Practically, dispersion is placing the CBA upon or adjacent to a target immediately before dissemination, so that the material is most efficiently used, and would at its maximum reach

the opponent. The act of dispersing takes place as a result of explosion of the munition, or otherwise thanks to collateral mechanical devices that generate air, inert gas or liquid propellant. Concomitant aerosolisation of the concerned CBA would enhance its dispersal and effectuality. Basically, CBW delivery methods fall into two broad categories: line sources and point sources. Line source delivery involves dispersing an agent from a moving source that can cover a much larger area than point source delivery would. Line source delivery systems include sprayers attached to moving aircraft, vessels, or vehicles. Point source delivery involves dispersing an agent from a single location. Point source delivery systems include grenades, mines, artillery shells, aerial bombs, rockets and warheads delivered via missiles. Basically, CBW delivery methods fall into two broad categories such as line sources and point sources:

- Line source delivery – involves dispersing an agent from a moving source that can cover a much larger area than point source delivery would. Line source delivery systems include sprayers attached to moving aircraft, vessels, or vehicles.
- Point source delivery – involves dispersing an agent from a single location. Point source delivery systems include grenades, mines, artillery shells, aerial bombs, rockets and warheads delivered via missiles.

In dissimilarity to the above described delivery modes, commandos or terrorists can use CBWA via standardised or improvised small devices, at times quite simple and yet effectual, or even just contaminate directly water and food consumed collectively or by certain persons. Aerial contamination, whether in a closed space or environmentally would chiefly rely on spraying devices, while the latter can serve for assassinations as well. Such operations may be carried out clandestinely or overly, including by suiciders. Chemical weapons[2] include toxic and non-toxic agents that have the purpose to kill or severely injure. Toxic agents are nerve agents such as sarin, soman, tabun, VX, GF, novichok agents, choking or lung-damaging agents such as chlorine and phosgene, blood agents also called asphyxiants such as hydrogen cyanide, cyanogen chloride, arsenic compounds and blister agents or vesicants such as sulfur mustard, nitrogen mustard, lewisite, phosgene oxime. Non-toxic agents impair human functioning and can be grouped into incapacitating agents aiming to temporarily incapacitate such as central nervous system stimulants, like amphetamines, central nervous

[2] USAMRICD 2000.

system depressants like opioids, psychedelics like LSD-25 and deliriants like BZ. Malodorants are disgusting and smelly odorants. The idea behind is to combine several stinking substances that are largely based on sulfur, as one example, along with a sniffing factor that will spray and cause nausea and escape. The difficult military experience of the U.S. military in Somalia has led to the use of such substances. Another example is the mixture named 'Skunk', which contains an organic and non-toxic blend of baking powder, yeast and other ingredients. There are also partially incapacitating agents such as vomiting agents like adamsite, and irritant agents also called lacrimators like CS or tear gas. Exposure or contact with an agent does not necessarily lead to absorption, namely penetration of the epithelial barrier. Contact with epithelial tissues may include skin, lungs, eyes and gut, and may lead to percutaneous absorption, inhalational absorption, ocular absorption, or enteral absorption, respectively. When absorption does occur, consequential effects might be limited to the site of contact, or much wider, due to systemic distribution of the toxic molecules in the body. An area denial weapon or anti-access/area denial weapon system is a defensive device or strategy used to prevent an adversary from occupying or traversing an area of land, sea or air. Alongside, the massive use of defoliants or herbicides such as Agent Orange, which contains the toxic element dioxin known from the Vietnam War, can be regarded as an effectual interdiction measure, because they leave areas empty of any form of vegetation cover. In the desert-like terrain that ensues, it is impossible for the enemy to travel without being seen, and there is little cover in case of an attack, especially from the air. White phosphorus munitions may cause significant toxic effects in high concentration, hence can at time be used as a substitute. CWA constituting power multipliers through attacking non-living targets during hybrid warfare might include a variety of substances that:

- block vital openings
- eat away the insulating materials of electrical wires
- are corrosive towards rubber
- can betray the vehicles to the radar
- cause vehicles to slip; neutralise essential lubricants

The domain of biological weapons (BW) is more complex than the domain of CW, although there are various significant common denominators. The way BW are presented hereafter is hence rather different from CW. BW are most outstanding in general, in that technologically the needed a shift from producing defensive biologicals, in that case vaccines to offensive biological

weapons agents (BWA) is minimal, an attribute bearing multiple implications, including in the dimension of hybrid warfare. Moreover, BW are the only weapons either within the context of unconventional or conventional warfare that in principle mimic natural phenomena in the form of infectious diseases, hence are highly disguisable, potentially, when employed clandestinely. BWA include, basically, pathogens and toxins that may be classified into live, hence reproducing agents/pathogens and nonviable agents/toxins:

- toxins – include ricin, botulinum, mycotoxins
- viral diseases – include SARS, Marburg and smallpox
- bacterial diseases – include anthrax, cholera and brucellosis
- fungal diseases – include histoplasmosis
- lethal or sub-lethal agents – that do not present themselves to a clear-cut classification, since mortality rate may widely vary
- transmissible or contagious agents – also called epidemic pathogens or non-transmissible pathogens

Natural or modified/engineered pathogens and toxins abruptly in the case of toxins or gradually in the case of pathogens affect the target such as humans, husbandry, crops, or materials. The vehicle may be natural (infected insects, animals, or human beings) or artificial (warheads, aerial bombs, artillery shells, man-made disseminators, i.e. sprayers, including through guerrilla warfare). The route of penetrating the body is the respiratory system, alimentary tract, eyes or rarely skin. It seems, then, as if the most significant distinctions can be made between epidemic and non-epidemic agents on the one hand and independently, between treatable and untreatable agents, on the other. Although the former distinction relates equally to bacterial and viral pathogens, the latter reflects a fundamental difference between those two major classes. Regardless of anti-sera, antiviral preparations are of limited efficacy, although they are expectedly being upgraded. Vaccines, as prophylactic measures, are in principle efficient against viruses, bacteria and protein toxins. The impact of BW employment is appreciably varied, both spatially and temporally. Its variability is shaped by the following factors:

- initial area coverage – the primary area contaminated, via air, water supplies, food supplies, or animal vectors/carriers
- contagiousness – is vital to attain epidemicity and thereby a much wider affected area, for example plague

- demographic conditions – population density would significantly extend the chain of infection range
- climatic conditions – sunlight in the form of ultraviolet light would usually damage the BWA, but wind might enlarge affected area
- duration of pathogenetic course – from hours in the case of toxins to weeks in the case of SARS, or even longer periods
- curability – by antisera if available against toxins, bacteria, or viruses or by antibiotics against bacteria
- environmental stability of the pathogen/toxin – of utmost stability are anthrax and mycotoxins
- conduction and effectiveness – of preventing measures before and after the act of BW employment

Beyond BWA affecting humans, should be mentioned BWA attacking husbandry such as foot and mouth disease virus and BWA attacking crops such as stem rust fungus. BWA attacking non-living objects are bacteria naturally or genetically engineered able to feed and eat various key substances. The latter include plastics, rubber, asphalt, fuel and oil. Area denial BW are spores that can contaminate the ground for lengthy periods of time, thanks to their superb endurance, thus providing a form of area denial. Other biotic force multipliers are cybernetic organisms, and bio-robots are being developed as components of hybrid warfare that have meaningful impacts. Notably, such fighting vectors were recently underscored by far in a RAND report prepared for the Pentagon.[3]

Preparedness and precautionary measures

CBW preparedness is a research-based set of actions that are taken as precautionary measures in the face of CBW threats and impacts. The latter include:

- personal illness that may lead to death of soldiers and/or civilians
- incapacitated manpower
- logistic efforts needed to medically support and isolate the infected/sickened victims
- meticulous, extremely demanding managing of the apparently unaffected population

[3] Matthews et al. 2024.

- demoralisation that may ascend to total panic
- economic crisis
- overall instability[4]

CBW preparedness is a major phase of CBW emergency management and an important quality in achieving related goals and in avoiding and mitigating damaging impacts. A fundamental distinction would be needed between CBW threats that concern civilian targets or military targets. The most developed type appears to be 'disaster preparedness', defined by the UN as involving "forecasting and taking precautionary measures before an imminent threat when warnings are possible".[5] CBW preparedness is initially propelled by an intelligence assessment posing either a potential or concrete CBW threat. The methodology of creating CBW preparedness includes the exploration of theoretical, possible and feasible scenarios of threat materialisation, intelligence monitoring, potential or concrete threat assessment of adversaries' efforts, capabilities and intentions, planning of the corresponding emergency management alignment, education, practising and periodical training. Within that context, a potential threat is observed as an actual effort to procure CBW, whether through a domestic program of research, development and production, or from extraneous sources. A concrete threat is observed as an existing CBW already possessed by an adversary that might have intentions to employ them. At that point, an intelligence endeavour to explore whether and in what modes a given CBW threat is prone to materialise in whatever form of hybrid warfare is crucial. Afterwards, persistent intelligence aiming at continuously monitoring the adversary's doctrine that involves CBW within hybrid warfare scenarios is vitally needed. The intelligence components involved include:

- analysis of exports and imports of single-use and dual-use chemicals and equipment
- human intelligence such as diplomatic, refugee and spying reports (HUMINT)
- photography from satellites, aircraft and drones (IMINT)
- examination of captured equipment (TECHINT)

[4] Shoham 2007.

[5] Kent 1994: 11.

- communications intercepts (COMINT)
- detection of chemical manufacturing and chemical agents themselves (MASINT)

Thus once established, a certain CBW threat would imperatively lead to a phase of threat management. Beyond the cardinal component of intelligence, that phase may include efforts to defy the forming of threat, a counter-doctrine of retaliation in kind or otherwise, and the orderly resultant construction of an emergency management alignment. The latter would usually be divided into an upon-threat-materialisation-crisis management sub-alignment, and a post-threat-materialisation management sub-alignment. It would rely on practical capacities of detection of chemical attacks ideally preceded by intelligence warning, specific identification of CBAs, individual protection such as gas masks, clothing, antidotes, anti-sera, vaccines, anti-microbial drugs, collective protection, building/shelters protection, decontamination, evacuation, hospitalisation and medical treatment. As a principle, particular military procedures, which are usually the model for civilian procedures, depend on the equipment, expertise and personnel available. The United States' (U.S.) approach is essentially whole community preparedness (in reference to the civilian sector): "By working together, everyone can keep the nation safe from harm and resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics."[6] CBW threats either within the context of terrorism or military unconventional attacks are equivalents. The U.S. Federal Emergency Management Agency, individuals, families, businesses, faith-based and community groups, profitable groups, schools and academia, media outlets, and all levels of governments are to take an active role in preparedness efforts. A disaster will affect the whole community, so everyone must be ready, by making a plan, being informed, and taking action to mitigate the effects of future crises. A most grand program aiming to scale up preparedness to bioterrorism was based on the U.S. Project Bioshield Act, which was passed by the Congress in 2004. The Act called for $5 billion to purchase vaccines that would be used in the event of a bioterrorist attack. In its full amplitude, the program was designed to acquire medical countermeasures to biological, chemical, radiological and nuclear agents for civilian use. Actually, since the 2001 terrorist attacks against the Twin Towers and the anthrax letters,

[6] *GeoCONOPS Alignment to Federal Doctrine: PPD-8* s. a.; U.S. Department of Homeland Security 2015.

the U.S. has allocated nearly $50 billion to address the threat of biological weapons. The U.S. funding for bioweapons-related activities focuses primarily on research for and acquisition of medicines for defence. Funding also goes toward stockpiling protective equipment, increased surveillance and detection of biological warfare agents, and improving state and hospital preparedness.[7] The corona pandemic and the possibility that the virus was developed as a BWA and accidentally leaked in Wuhan added an amplified dimension. Thus, the U.K. established in 2023 the *UK Biological Security Strategy.*[8] Further, underpinned by the UK Biological Security Strategy and the U.S. Biodefense Strategy, the U.S.–UK Strategic Dialogue on Biosecurity took place in January 2024 and reflected a shared ambition to protect against a growing and diverse spectrum of biological threats. These threats include future pandemics, antimicrobial resistance, a deliberate bioweapon attack, as well as those that might arise from the misuse of biotechnology.[9] Moreover, the World Economic Forum recently launched the Biothreat and Disease Surveillance Initiative to catalyse the establishment of public–private collaborations that improve the capacity to prepare and respond to biological threats.[10]

Hybrid warfare with CBW

During the eight-year Iran–Iraq War (1980–1988), more than 350 large-scale Iraqi chemical attacks were reportedly conducted since 1982 in the border areas, and took place until the last day of war. Most of the chemical attacks were combined with conventional Iraqi attacks, and played a highly important role in Iraq's military success. Essentially, the Iranian forces were most of the time unprotected, and Iran did not possess any CBW at that time, to retaliate with. Hybrid warfare is low risk, low cost and provides an adversary the opportunity to obfuscate, throwing doubt on who is responsible for gray zone actions. Thus, the Syrian regime's use of CW during the Syrian Civil War (since 2012) has been a lasting illustrative example in that an indicator that the regime might be about to use CW would be planting information that the opposition has CW. Then,

7 Gottlieb 2013.
8 Cabinet Office 2023.
9 East–Regan 2024.
10 Shapiro – Du Moulin 2024.

when there is chlorine in some Syrian village, who is to say it came from a barrel bomb? This type of tactic might be a particular problem with consensus-driven organisations, such as NATO.[11] Moreover, after the Syrian-declared CW arsenal was destroyed, the Syrian regime persistently claimed it does not possess CW while concurrently hiding and often employing significant portions of the real arsenal as a disinformation line aiming to refute Syrian CW employment. An additional line of Syrian disinformation warfare has been the concurrent elimination of evidence indicating that CW were used.[12] The concrete mechanism of Assad's decision-making in relation to the transition from conventional to CW is not clear. It can be assumed that he is the authority approving that transition, at least in those cases where sarin was employed, which is not necessarily the case with chlorine. The Syrian regime's desire to use CW has stemmed largely from its inability to achieve or major difficulty in achieving, various tactical, operational and strategic goals either military or demographic by means of conventional weapons. This was a chief drive behind Syria's retention of sarin.[13] Thus, the Syrian regime was highly predisposed to employ CW in numerous occasions during the war, but considerable international pressure as opposed to concurrent backing, if indirect yet solid lent by the Russians and the Iranians posed unignorable restrictions. Obviously, the Syrian CW arsenal has not been dismantled. Thus, the Syrians once and again had two decisions to make: whether to employ CW and what type of CWA to choose given that the Islamic State of Iraq and Syria, better known as ISIS or any other group never possessed nerve agents, hence cannot be accused of using such CWA. Therefore, the Syrian Army mostly used chlorine gas and only in a few cases sarin, still endeavouring though to trickily obfuscate, contemporarily. Within that context, the first employment of sarin by the Syrian Army in Khan al-Asal in March 2013, was a typically complicated event of hybrid warfare.[14] Several further employments of sarin by the Syrian Army were conducted until 2018. The last one in Douma in April 2018, was followed by American–British–French retaliatory raids against Syrian CW facilities. Interestingly, in a statement condemning the 2018 Western raid, Russian Foreign Minister Lavrov said: "We told the USA where our red lines were, including the geographical red lines, and the results have shown that they

[11] Garamone 2019.
[12] Shoham 2015a.
[13] Shoham 2017.
[14] *Khan al-Assal Chemical Attack* s. a.; René–Domingo 2014.

haven't crossed those lines."[15] Beyond, however, disinformation warfare did follow the U.S. strike. On 11 April 2018 Putin suggested the chemical attack was a false flag operation intended to discredit the Syrian Government. On 13 April 2018 President Assad said the attack was "100 per cent fabrication" by the United States "working hand-in-glove with the terrorists", intended to provide a pretext for the airstrike on the Shayrat Airbase.[16] In an unprecedented television interview, on *Russia Today* in May 2018, Syrian President Assad posed detailed argumentation (ostensibly) for his army's alleged non-use of CW. Referring to the (confirmed) employment of sarin in Duma and the subsequent American–British–French retaliatory raid, Assad claimed that CW had not been used by anyone, (rather than by the rebels or other groups) as has usually been contended by Syria.[17] The Russo–Ukraine War, which started in February 2022 is a conventional warfare conjoined with concomitant CBW-related elements. Since the beginning, a remarkably eventful information and intelligence dialogue evolved between Russia and the U.S., marking a hybrid warfare that involved Russian moves in Ukraine connected with significant concomitant CB elements, though not concrete employment of. On 24 February, the day the Russian invasion started Lieutenant General Igor Kirillov, Chief of the Nuclear, Biological and Chemical Protection troops of the Russian Army said that documents uncovered by the Russian military in Ukraine "show that the Ministry of Health of Ukraine has set the task of completely destroying bio-agents in laboratories. The Pentagon knows that if these documents fall into the hands of Russian experts, then it's highly likely that Ukraine and the United States will be found to have violated the BW Convention." China subsequently backed the Russian claims.[18] The U.S. said in response that its pertinent program does the opposite and in fact aims to "reduce the threat of biological weapons proliferation". Contemporaneously, the WHO "has strongly recommended to the Ministry of Health of Ukraine and other responsible authorities to destroy the dangerous pathogens in order to prevent any possible leakage".[19] Some days earlier, within a CW context, a Russian Ministry of Defence briefing on 11 May asserted that Ukrainian forces had "carried out an explosion of a tanker with fertilizer, presumably ammonium nitrate, which

[15] Shoham 2018a.
[16] Shoham 2020.
[17] Shoham 2018a.
[18] Rising 2022.
[19] Lanese 2022.

resulted in a cloud of orange smoke that dissipated after some time". According to Moscow, the aim of the explosion, which occurred in the Kharkov region, was to accuse Russia of using CW in order to "extract additional military aid from the West by the Kyiv regime".[20] Besides, on several occasions during the war, the Russian Army was accused of using white phosphorus munitions such as toxic smoke not defined as CW and it is likely that at least in one case it was indeed used. Nevertheless, multiple cases in which riot control and irritant chemical agents – possibly including novel versions – were employed by the Russian military, have apparently been evidenced.[21] All in all, the context at large, and the chronology detailed, are emblematic of a modern conflict that is hybrid in nature, and potentially harboured imminent CBW-related threats.

Chemical and biological terrorism

Since its emergence ISIS has sought CW and has used them, mostly chlorine and rarely mustard, against its opponents, namely Syrian government forces, the Syrian opposition groups, Kurds and Iraqis. Usually, CW employment was synchronised with conventional warfare in a bordering territory.[22] The Sarin attack in the Tokyo Metro was an act of chemical terrorism perpetrated in March 1995 by members of the domestic Japanese cult movement Aum Shinrikyo, a basically religious group. In five coordinated attacks, the perpetrators released nerve agent sarin on three lines of the Tokyo Metro during the rush hour, killing 14 people, severely injuring 50 some of whom later died, and causing temporary vision problems for nearly 1,000 others. The attack was directed against trains passing close to the location of the Japanese parliament headquarter. The nerve agent was produced by the cult in Japan. It was released inside the train by puncturing plastic bags containing it and carried by the perpetrators. The perpetrators were caught later on. The attack was regarded by the attackers as an "act of salvation".[23] St. Luke's International Hospital in Tsukiji was one of very few hospitals in Tokyo at that time to have the entire building wired and piped for conversion into a 'field hospital' in the event of a major disaster. This

[20] Coleman–Devlin 2022.
[21] Kyiv Post 2023.
[22] Shoham 2015b.
[23] *Tokyo Subway Sarin Attack* s. a.

proved to be a very fortunate coincidence as the hospital was able to take in most of the 600+ victims, resulting in no fatalities. As there was a severe shortage of antidotes in Tokyo, sarin antidote stored in rural hospitals as an antidote for herbicide/insecticide poisoning was delivered to nearby stations, where it was collected by a Ministry of Health official on a train bound for Tokyo.[24] Russian ex-intelligence Colonel Sergei Skripal and his daughter Yulia were found in March 2018 unconscious on a public bench in London, due to Novichok nerve agent intoxication, conducted by Russian secret agents. Skipal has been recruited to British intelligence, and passed on state secrets and blew the cover of numerous Russian agents.[25] Well characterised, "the event in Salisbury wasn't an isolated incident. It was part of a wider coordinated strategy to exert power and influence in a new era of warfare. Often termed 'hybrid warfare', the strategy sits outside of the typical rules-based system of traditional foreign policy. It is a doctrine that is highly flexible and adaptive; it uses a variety of covert tools at its disposal to achieve strategic political objectives."[26] In this specific case thus, the poisoning task was but one quite drastic element within a broad range of Russian intelligence plus counterintelligence warfare. The Russian foreign ministry's denials were implausible. This was an example of Vladimir Putin's hybrid warfare, or probably what's better described as 'hybrid politics'. He's willing to use Russian power in transparent ways and trust that responses will be ineffective or require long processes that he can frustrate. The initial Russian response to the U.K.'s request for an explanation has been to deny any knowledge or involvement, and to request more details. Russian spokespeople have also started to provide 'alternative facts' about the attack, even speculating that it could have been conducted by U.K. authorities to discredit Russia.[27] Typically Russian disinformation warfare that followed an event combining intelligence warfare and chemical terrorism warfare. And yet, this assassination attempt was just one of multiple cases combining individual chemical terrorism warfare, intelligence warfare and disinformation warfare, as follows. Viktor Yushchenko, President of Ukraine from 2005 to 2010 was poisoned in Ukraine, likely by Russian agents during his election campaign in September 2004. He was flown to Vienna for treatment and diagnosed with several syndromes, due to a serious viral infection

[24] Smithson–Levy 2000.
[25] Shoham 2018b.
[26] Balson 2021.
[27] Shoebridge 2018.

and a toxic chemical substance called dioxin, which is not normally found in food products. After the illness, his face was greatly disfigured. A former Russian Federal Security Service officer who specialised in tackling organised crime, Litvinenko publicly accused their superiors, in November 1998, of ordering an assassination of a Russian tycoon. Litvinenko was arrested and afterwards fled in 2000 to London, where he was granted asylum. There, he worked as a journalist, writer and consultant for British intelligence. During his time in London, he wrote two books, wherein he accused the Russian secret services of staging several acts of terrorism in an effort to bring Vladimir Putin to power. In November 2006, Litvinenko suddenly fell ill and was hospitalised in what was determined to be a case of a lethal poisoning by radioactive Polonium-210. The intoxication was conducted by Russian secret agents. Notably, the methods of infiltrating the poisons from Russia into the U.K. and Ukraine constitute their own separate issue, which is of paramount importance. The political assassination with nerve agent VX in February 2017 of North Korean ruler Kim Jong-un's estranged half-brother Kim Jong-nam in Malaysia, by North Korean agents warrants attention. Kim Jong-un most probably backed the murder.[28] Examples of biological terrorism are also remarkable. One week after the Twin Towers plus Pentagon events, five regular letter envelopes containing anthrax (Ames strain) spore powder were mailed from New Jersey (NJ) on 18 September 2001 to news media reporters in the U.S. and two additional anthrax letters were mailed from NJ on 9 October 2001 to two Senators. Most of the envelopes were opened without control. Twenty two people were infected and five died. According to the FBI, the ensuing investigation became "one of the largest and most complex in the history of law enforcement".[29] Overall, dozens of buildings were contaminated with anthrax due to the upgraded floatability of the structured powder as a result of the first five mailings, which contained, altogether about 18 gr. of the sabotage spore powder. The decontamination of the Brentwood postal facility took 26 months and cost US$130 million. The Hamilton, NJ postal facility remained closed for 41 months (its cleanup cost US$65 million). The Environmental Protection Agency spent US$41.7 million to clean up government buildings in Washington, D.C. One FBI document said the total damage exceeded US$1 billion. The 22 cases that comprised the American Anthrax Outbreak of 2001 likely had contact with one or more of seven spore-laden envelopes.

[28] Shoham 2018c.
[29] Shoham 2007.

But the anthrax letters affair was not limited to the U.S. The American embassy in Vilnius, Lithuania was likewise concurrently targeted. For the time being, the culmination of bioterrorism worldwide has been this act of distributing mail envelopes containing anthrax spore powder. It reflected noticeable supremacy of a simple act of bioterrorism irrespective of preparing the anthrax powder in itself, which was very sophisticated in several senses:

- uncontrollable preparing of the postal envelopes containing the anthrax powder
- uncontrollable, repeated mailings
- undetectable conveying of the mailed envelopes until reaching their various destinations

An intermittent Pentagon report said "the anthrax attacks revealed weaknesses in almost every aspect of U.S. bioterrorism-preparedness. As simple as these attacks were, their impact was far-reaching."[30] It provided a detailed and informative but hardly unsuspected inventory of shortcomings in emergency preparedness and response. Following a zigzag investigation the FBI concluded that Bruce Irvine, an anthrax scientist from the U.S. Army Medical Research Institute of Infectious Diseases was the culprit. However, this assertion has been widely doubted while a feasible alternative pointed to Iraq being the provenance of remarkably advanced sabotage spore powder and al-Qaeda being the implementer. A highly potent biotoxin, ricin can easily be derived from castor beans, which was indeed the case in actuality with reference to various terrorist groups, including al-Qaeda. On two occasions in the U.S., envelopes containing ricin were mailed to the White House in November 2003, and to the U.S. Senate Office of the Majority Leader in February 2004. Much earlier in 1978 Georgi Markov, a Bulgarian regime opponent, was assassinated in London with ricin through collaboration between Soviet and Bulgarian secret services. In the Moscow Theater in October 2002 an incapacitating agent was used and markedly decreased alertness and clarity, caused drowsiness, deep loss of consciousness, and even fatal coma in a closed space. It happened after Chechen terrorists took over the Moscow Theater. Between 40 to 50 armed Chechen terrorists seized about 800 hostages and ended with the death of at least 150 people, mostly due to intoxication.[31] The Russian security services pumped an aerosol anaesthetic, later stated by

[30] Shoham 2007.
[31] CNN 2002.

Russian Health Minister Yuri Shevchenko to be based on fentanyl, into the theater through the air conditioning system. The discovery caused panic in the auditorium. Fentanyl is a powerful opioid used as a pain medication. Actually, an undisclosed incapacitating agent was used by the Russian authorities in order to subdue the Chechen terrorists who had taken control of the crowded theater. A later meticulous investigation revealed that the agent used was a mixture that contained two fentanyl derivatives much stronger than fentanyl itself, sprayed in an aerosol mist, namely the opioids carfentanil, which is a large animal tranquilizer and remifentanil, a surgical painkiller).[32] The pertinent chemical warfare agent has been designated by the Russians Kolokol-1. The event was potentially catastrophic, in that it seems likely that the 800 hostages were about to be killed by Chechen rebels. To rescue them, the Russian military used a calmative agent in an attempt to subdue the rebels. Overall, the case is highly demonstrative of a commercially distributed substance which may be, or is readily adopted as a typical CW. Hybrid threats of indirectly induced CB impacts can include destruction/sabotage by conventional warfare of domestic CB facilities including completely civilian ones in order to cause leakage and environmental CB contamination. Cyber operations aimed to generate uncontrolled above-standard CB contamination happened in May 2020, when an Iranian cyberattack on Israel's drinking water systems aimed to destabilise the chlorine level and poison the country's citizens. Iran was behind the attack, with hackers using American servers to carry out the breach, which somewhat affected several water facilities throughout Israel. Intensive disinformation warfare by Iran followed the event.[33] Particularities of the SARSCoV2 pandemic within the context of hybrid warfare are linked to the complexity of the debate over the origin of the pandemic virus, whether it was a natural scenario or a lab accident. Accidental leak of a lab-designed virus could take place during a scientific public health program and/or a military program. The debate is challenging, and is at any rate conjoined with hybrid warfare. Connectedly, one intriguing possibility which is here inquired into, among others, is the approach posed by a former U.S. State Department principal investigator who officially dealt with this matter, Dr. David Asher, in reference to China's strategy at large: "The Chinese have made it clear they see biotechnology as a big part of the future of hybrid warfare.[34] […] We didn't

[32] Riches et al. 2012.
[33] I24 News 2020.
[34] Birrell 2021.

come at this saying: Let's go blame the Chinese. But we […] had to appreciate the nature of the Chinese government. This is a government that since 2007 has been writing publicly about genetic warfare. […] The Chinese government, at the leadership of the People's Liberation Army (PLA), and even at Xi Jinping's level himself, have at least suggested that bio war is the future of war in some ways, even going beyond nuclear war. I don't know quite what that means, but when I start to read that in publications which are not classified but not well read because they're in Chinese and they're aimed at a Chinese audience, you start to say, "What are they talking about?" […] On Chinese national TV [in 2017], there was an interesting media commentary by their lead PLA commentator about that, [saying] "we have entered into an area of Chinese bio warfare, including using things like viruses." I mean, they made a public statement to their people that this is a new priority. […] You need to understand the context of Chinese hybrid warfare. You need to understand the nature of the communist state in China, and its secretive dual use approach to everything military, to be able to appreciate it."[35] Practically, China has been accused of:

- gain of function experimentation much beyond the norms
- responsibility for an accidental pandemic virus leakage
- reporting about the epidemic outbreak much after real time
- reporting that the virus is non-transmissible among humans
- allowing flights from China outwards as usual
- hiding data concerning the genomic origin of the virus and direct source of the initial human infection

In connection to the above, and referring to the Annual Threat Assessment of the U.S. Intelligence Community of 7 February 2022, it is worth noting within the BW dimension the following:[36]

- "Global shortcomings in preparedness for the pandemic and questions surrounding the origins of the Covid-19 virus and biosecurity may inspire some adversaries to consider options related to biological weapons developments.
- As China, Iran, and Russia continue to publicly tout individual or collaborative efforts to improve biosecurity, they have pushed narratives that further drive threat perceptions, including linking U.S. laboratories

[35] Asher–Yu 2021.

[36] Office of the Director of National Intelligence 2022.

abroad to Covid-19 origins, breaches in biosafety, untrustworthy vaccines, and biological weapons. This messaging probably will be amplified in the lead up to the once-every-five-years Review Conference of the Biological and Toxin Weapons Convention, tentatively slated to convene in mid 2022.
– Rapid advances in dual-use technology, including bioinformatics, synthetic biology, and genomic editing, could enable development of novel biological weapons that complicate detection, attribution, and treatment."

Connectedly, if in a collateral manner, it is of note that since the Covid-19 period, health sectors have become a favourite target for all types of cyberattacks in the entire world.[37] Further, the dimension of unrestricted hybrid warfare within the context of militarily manipulated biotechnology – combined with formation of solid footholds in the territory of the adversary (or ostensible partner), as well as with massive scientific espionage – has been materialised by China in effect, in the U.S.,[38] Canada[39] and Europe.[40] Far beyond, the issue of ethnic/biogenetic weapons is intriguing; the excludability of its feasibility appears to be uncertain. It so happened that in 2007, when China institutionalised its doctrine in that uncanny arena (as mentioned above) it was reported that the Russian Government banned all exports of human biosamples, while the reason for the ban was allegedly an account by the head of the FSB Nikolay Patrushev presented to Vladimir Putin. The account claimed about on-going development of "genetic bioweapons" targeting the Russian population by American and Polish institutions, including the Institute of Genetics and Biotechnology, Warsaw University and the Department of Medical Biotechnology, Jagiellonian University;[41] seemingly an earlier version of the bio-information warfare that reappeared 15 years later around Ukraine, as described. On the whole, China, Russia, Iran and North Korea certainly possess stockpiles of BW, and pose potentially serious biothreats. Particularly, China's conduct is implicative of unexplained peculiarities prior to, especially towards, and after the start of the pandemic, joined together with a variety of disinformation and misinformation warfare.[42]

[37] Remarks by the Head of the National Cyber System Gabi Portnoy at the Ministry of Justice; notification by the National Cyber Array, Israel, 26 October 2022.
[38] Sellin 2022a; Sellin 2022b.
[39] Shoham 2019.
[40] Sellin 2022c.
[41] Kommersant 2007.
[42] U.S. Senate 2022; Office of Senator Marco Rubio 2023.

Conclusion

The sphere of CBW, although representing mighty weapons of mass destruction on their own, constitutes a highly meaningful vector within the doctrine of hybrid warfare. A diversified spectrum of CBW is liable to meet that was presented in this chapter, together with a variety of actual events and feasible scenarios. This expounds the complicatedness and effectiveness of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers. Such modes, both tactically and strategically, have already been repeatedly implemented in reality as detailed, and are prone to expand. CBW may typically constitute a game changer in hybrid warfare either as a meaningful force multiplier of another main effort warfare, or as a main effort in itself amplified by another concurrent warfare serving as a force multiplier. A significant characteristic is the considerable modularity marking the pertinent interfaces, in that the lowest level of purposive coupling of CBW is with another warfare mode serving to facilitate or amplify the CBW effect, such as concurrently destroying warehouses storing protective CBW equipment. A higher level of purposive combining is with simultaneous invasion of CBW-protected infantry forces destined to defeat the CBW-afflicted enemy, occupying the territory held by the enemy. And so forth can be added at the same time or slightly later further layers of other warfares aiming either to increase the effectiveness of the three above mentioned elements, or to serve for a far higher broader purpose, which is still being assisted by those three elements as well. In a way, it is possibly an orchestration scaled up, contemporaneously, from tactic levels to strategic levels. Alongside, intelligence warfare is fundamentally a unique type of permanently ongoing warfare, including the CBW domain in terms of both intelligence and counterintelligence. Thus, CBW intelligence warfare is being conducted continuously on a basic level, as well as towards CBW employment, hybridly, during CBW employment, and increased when CBW defensive preparedness is heightened. Disinformation warfare and deception are often conducted verbally and/or practically together with CBW employment, aiming to obfuscate evidence, suspicions, or assessments related to the employer identity. Such a hybrid warfare might be sophisticated, challenging and at times entirely effective. Moreover, natural occurrences of toxins and of pathogens may serve as camouflage for BWA employment, thereby enabling efficient hybrid warfare. Remarkably, as shown, CBW are not designed against humans merely. A variety of CBWA are intended for attacking farm animals, crops, wild vegetation or defoliants,

and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare. On the whole, the CBW dimension of hybrid warfare is highly consequential. It has already proved as such along a wide diversity of events that took place in effect as detailed, while further, various scenarios embody considerable feasibility to happen in actuality. Basically, they might be implemented hybridly and flexibly as impactful components, through a wide range of options.

Questions

1. What are the singularities of CBW as weapons of mass destruction?
2. How can you explain the meaningfulness of CBW as a vector within the doctrine of hybrid warfare at large?
3. What is the consequentiality of the category termed 'Unrestricted Hybrid Warfare', foremost conceptualised and upgraded by China and Russia?
4. What is the actuality of events and feasible scenarios, which expound the complicatedness and impacts of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers?
5. How can one typologically and detailedly expound this coupling, so as to enhance preparedness and countering capacities?
6. What are the utilities of CBW in hybrid warfare beyond anti-human effects, namely for attacking farm animals, crops, wild vegetation (defoliants), and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare?
7. What is the weight of a nearly existing horizon of hybrid warfare apt to combine conventional warfare modes together with new generations of a variety of by far advanced CBW?

References

Asher, David – Yu, Miles (2021): Transcript: The Origins of Covid-19: Policy Implications and Lessons for the Future. *Hudson Institute,* 17 March 2021. Online: www.hudson.org/foreign-policy/transcript-the-origins-of-covid-19-policy-implications-and-lessons-for-the-future

Balson, David (2021): Tackling Hybrid Warfare: The Salisbury Poisoning Three Years On. *Ripjar,* 8 March 2021. Online: https://ripjar.com/blog/tackling-hybrid-warfare-the-salisbury-poisoning-three-years-on/

Birrell, Ian (2021): Worrying New Clues about the Origins of Covid: How Scientists at Wuhan Lab Helped Chinese Army in Secret Project to Find Animal Viruses. *The Mail on Sunday,* 24 April 2021. Online: www.dailymail.co.uk/news/article-9507749/How-scientists-Wuhan-lab-helped-Chinese-army-secret-project-animal-viruses.html

Cabinet Office (2023): *UK Biological Security Strategy.* Policy Paper by the U.K. Government, 12 June 2023. Online: www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html

CNN (2002): Chechen Gunmen Seize Moscow Theater. *CNN,* 24 October 2002. Online: https://edition.cnn.com/2002/WORLD/europe/10/23/russia.siege/index.html

Coleman, Alistair – Devlin, Kayleen (2022): Ukraine Conflict: Russian Chemical Attack Claim Fact-checked. *BBC News,* 15 May 2022. Online: www.bbc.com/news/61439398

East, Christopher – Regan, Dan (2024): Event Summary: the U.S.–UK Strategic Dialogue on Biosecurity. *Council on Strategic Risks,* 22 January 2024. Online: https://councilonstrategicrisks.org/2024/01/22/event-summary-u-s-uk-strategic-dialogue-on-biosecurity/

France 24 (2022): Ukraine Accuses Russia of Using Phosphorus Bombs in Fresh Strikes on Snake Island. *France 24,* 1 July 2022. Online: www.france24.com/en/europe/20220701-live-russian-missile-strike-on-apartment-building-in-odesa-kills-10

Garamone, Jim (2019): Military Must Be Ready to Confront Hybrid Threats, Intel Official Says. *U.S. Department of Defense,* 4 September 2019. Online: www.defense.gov/News/News-Stories/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intel-official-says/

GeoCONOPS Alignment to Federal Doctrine: PPD-8 (s. a.). Online: https://emilms.fema.gov/is_0060b/groups/17.html

Gottlieb, Scott (2013): Ricin, Domestic Bioterrorism, and the Lessons Learned After 9/11: Are We Safer Today Than We Were 10 Years Ago? *Forbes,* 17 April 2013. Online: www.aei.org/articles/ricin-domestic-bioterrorism-and-the-lessons-learned-after-911-are-we-safer-today-than-we-were-10-years-ago/

I24 News (2020): Report: Iran Behind Recent Cyberattack on Israel's Water Supply. *I24 News,* 7 May 2020. Online: www.i24news.tv/en/news/israel/1588852463-report-iran-behind-recent-cyberattack-on-israel-s-water-supply

Kent, Randolph (1994): *Disaster Preparedness.* Geneva: United Nations Disaster Management Training Program.

Khan al-Assal Chemical Attack (s. a.). Online: https://https://en.wikipedia.org/wiki/Khan_al-Assal_chemical_attack

Kommersant (2007): Russia Observes the Human Model. *Kommersant,* 29 May 2007.

Kyiv Post (2023): Ukraine Reports 465 Chemical Attacks by Russia Since Start of Full-Scale Invasion. *Kyiv Post,* 27 December 2023. Online: www.kyivpost.com/post/26011#:~:text=In%20December%20alone%2C%20Russian%20troops,grenades%20with%20unknown%20new%20agents

Lanese, Nicoletta (2022): Ukraine Should Destroy 'High-Threat' Pathogens, WHO Says. *Live Science,* 11 March 2022. Online: www.livescience.com/ukraine-labs-destroy-pathogens-who-advises

Matthews, Luke J. – Lee, Mary – De Bruhl, Brandon – Elinoff, Daniel – Eusebi, Christopher A. (2024): *Plagues, Cyborgs, and Supersoldiers. The Human Domain of War.* Santa Monica: RAND. Online: www.documentcloud.org/documents/24376031-rand_rra2520-1-1

Office of Senator Marco Rubio (2023): *A Complex and Grave Situation. A Political Chronology of the SARS-CoV-2 Outbreak.* 1 May 2023. Online: www.rubio.senate.gov/wp-content/uploads/_cache/files/4f6bb786-504e-443d-8904-974dafc1cd0e/CD3BC3317D197A25E9FF01EBFB869357.rubio-covid-origins-report-final.pdf

Office of the Director of National Intelligence (2022): *Annual Threat Assessment of the U.S. Intelligence Community.* Online: www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

René, Pita – Domingo, Juan (2014): The Use of Chemical Weapons in the Syrian Conflict. *Toxics,* 2(3), 391–402. Online: https://doi.org/10.3390/toxics2030391

Riches, James R. – Read, Robert W. – Black, Robin M. – Cooper, Nicholas J. – Timperley, Christopher M. (2012): Analysis of Clothing and Urine from Moscow Theatre Siege Casualties Reveals Carfentanil and Remifentanil Use. *Journal of Analytical Toxicology,* 36(9), 647–656. Online: https://doi.org/10.1093/jat/bks078

Rising, David (2022): China Amplifies Unsupported Russian Claim of Ukraine Biolabs. *AP News,* 11 March 2022. Online: https://apnews.com/article/russia-ukraine-covid-health-biological-weapons-china-39eeee023efdf7ea59c4a20b7e018169

Sellin, Lawrence (2022a): *The Great Link between the Netherlands and China.* Online: www.youtube.com/watch?v=D6SKBPFAJ0s

Sellin, Lawrence (2022b): *The Laboratory Origin of Covid-19 and the Ongoing Cover-up of its Origin, the Structure of China's Biowarfare Program and China's Massive Infiltration of U.S. Virus Laboratories.* Online: https://lawrencesellin.substack.com/p/the-laboratory-origin-of-covid-19

Sellin, Lawrence (2022c): *Chinese Biotech Firm with Deep Links to China's Military and Its Covid-19 Program just Bought Land in Florida for a Massive Research Complex.* Online: www.thegatewaypundit.com/2022/09/chinese-biotech-firm-deep-links-chinas-military-covid-19-program-just-bought-land-florida-massive-research-complex/

Shapiro, Molly – Du Moulin, Lora (2024): Lessons from Rwanda: Building Systems to Protect against Infectious Diseases and Biothreats. *World Economic Forum,* 22 January 2024. Online: www.weforum.org/agenda/2024/01/systems-infectious-diseases-biothreats-rwanda/

Shoebridge, Michael (2018): Russia, Novichok and the future of the Chemical Weapons Convention. *The Strategist, Australian Strategic Policy Institute,* 15 March 2018. Online: www.aspistrategist.org.au/russia-novichok-future-chemical-weapons-convention/

Shoham, Dany (2007): Bioterrorism. In Cox Gad, Shayne (ed.): *Handbook of Pharmaceutical Biotechnology.* Hoboken: John Wiley and Sons, 1525–1651.

Shoham, Dany (2015a): Syria's Chemical Weapon Obfuscations. *BESA Center Perspectives Paper,* (305), 7 August 2015. Online: https://besacenter.org/syrias-chemical-weapon-obfuscations/

Shoham, Dany (2015b): Does ISIS Pose a WMD Threat? *BESA Center Perspectives Paper,* (322), 13 December 2015. Online: https://besacenter.org/9562/

Shoham, Dany (2017): The Syrian Sarin Attacks of August 2013 and April 2017. *BESA Center Perspectives Paper,* (452), 26 April 2017. Online: www.jstor.org/stable/resrep04591

Shoham, Dany (2018a): Assad Addresses the Chemical Weapons Issue. *BESA Center Perspectives Paper,* (879), 1 July 2018. Online: https://besacenter.org/assad -chemical-weapons/

Shoham, Dany (2018b): Russia's Toxic Legacy. *BESA Center Perspectives Paper,* (792), 10 April 2018. Online: www.jstor.org/stable/resrep16934?seq=5

Shoham, Dany (2018c): The Peculiar Chronology of Persistent Nerve Agents. *BESA Center Perspectives Paper,* (912), 3 August 2018. Online: https://besacenter.org/persistent-nerve-agents/

Shoham, Dany (2019): China's Biological Warfare Programme and the Curious Case of Dr. Xiangguo Qiu. *CBW Magazine,* 12(4), Online: https://idsa.in/cbwmagazine/chinas-biological-warfare-programme

Shoham, Dany (2020): Syria's Chemical Arsenal: Obama's Failure, Trump's Mixed Success. *Middle East Quarterly,* 27(2), 1–8.

Smithson, Amy E. – Levy, Leslie-Anne (2000): *Ataxia: The Chemical and Biological Terrorism Threat and the US Response.* Online: https://cryptome.org/ataxia.htm

Tokyo Subway Sarin Attack (s. a.). Online: https://en.wikipedia.org/wiki/Tokyo_subway_sarin_attack#Attack

USAMRICD (2000): *Medical Management of Chemical Casualties Handbook*. U.S. Army Medical Research Institute of Chemical Defense.

U.S. Department of Homeland Security (2015): *National Preparedness Goal*. Online: www.fema.gov/sites/default/files/2020-06/national_preparedness_goal_2nd_edition.pdf

U.S. Senate (2022): *An Analysis of the Origins of the Covid-19 Pandemic*. Senate Committee on Health Education, Labor and Pensions, Minority Oversight Staff, October 2022. Online: www.help.senate.gov/imo/media/doc/report_an_analysis_of_the_origins_of_covid-19_102722.pdf