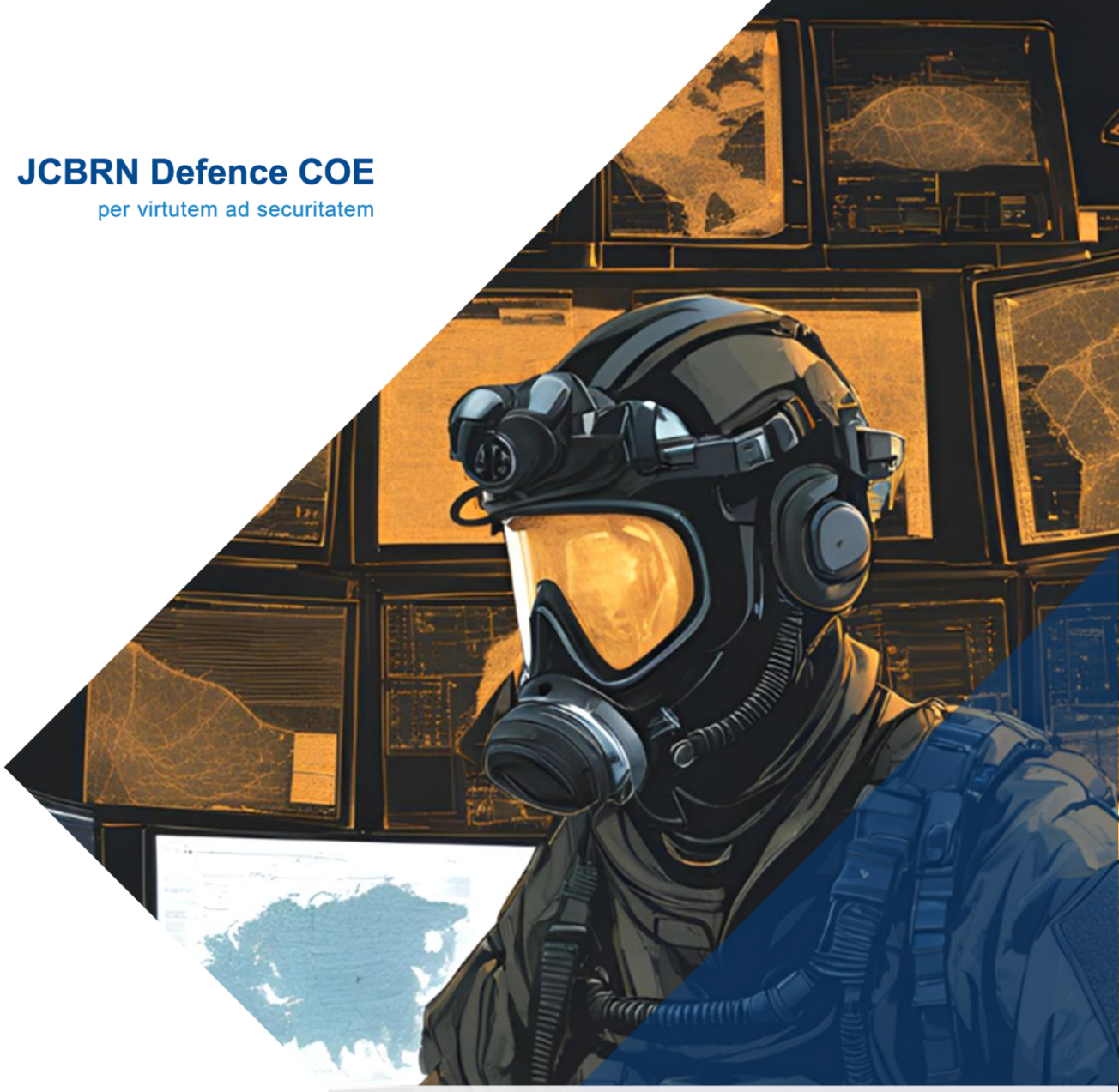
JCBRN Defence COE
per virtutem ad securitatem



# HYBRID THREATS IN THE CBRN ENVIRONMENT

## CHALLENGES AND IMPLICATIONS

**Paulina Frederike GOGACZ**

**Edited by Linda VAŘEKOVÁ**

2024

# Disclaimer

The publication reflects the author‘s positions, views, findings, interpretations and conclusions as an independent academic opinion. It is not a North Atlantic Treaty Organization (NATO) endorsed or approved document and does not reflect neither NATO‘s nor individual government‘s policies or positions nor does it reflect the policies or positions of the JCBRN Defence COE or its Sponsoring Nations and Contributing Partner. Although the JCBRN Defence COE has invested the utmost care in its preparation, the JCBRN Defence COE does not accept any liability for the accuracy and completeness of any information, instruction and/or advice provided, as well as for misprints. No claims can be made against the JCBRN Defence COE concerning potential consequences from the reliance on information or conclusions contained herein.



JCBRN Defence COE (2024): Bettering North Atlantic Treaty Organization‘s Combined Joint Chemical, Biological, Radiological and Nuclear Defence task Force with emerging and disruptive technologies.



*Cover image created using Canva AI Image Generator and used in accordance with Canva Text to Image Terms*

**JOINT CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE CENTRE OF EXCELLENCE**

Víta Nejedlého
682 01, Vyškov
Czech Republic

Phone: +420 973 452 777
IVSN: 925 4200 452 777
E-mail: postbox@jcbrncoe.org

**www.jcbrncoe.org**

www.twitter.com/jcbrncoe
linkedin.com/company/jcbrndefencecoe

# Executive Summary

**In the future, the convergence of threats and their amplification through threat multipliers is increasingly likely, as highlighted in NATO's most recent *Strategic Concept*. One example could be the proliferation of hybrid CBRN threats, where hybrid tactics are intentionally deployed in the CBRN environment. The terms hybrid warfare and hybrid threats originated in the early 2000s. Hybrid threats blend military, and non-military means to destabilise and undermine an opponent. Hybrid threats are difficult to attribute yet executed with intent, targeting societies to create confusion, disrupt decision-making, and sway public opinion. When combined with CBRN threats, they can significantly magnify the impact or hinder the response to such incidents.**

**Strategic documents from both NATO and the EU have acknowledged the significance of hybrid and CBRN threats. While both organisations recognise the need to address hybrid threats in the CBRN context, there are differences in their focus, scope of cooperation, and integration of hybrid threats into their CBRN frameworks to enhance respectively resilience and capabilities. Whereas NATO has already hinted at a "nexus" of these two threats, the EU has identified the absence of such an interconnected approach as a shortcoming in one of their assessments.**

**In recent years, CBRN threats have intensified due to the increased accessibility of materials and the comparable ease of producing and transporting CBRN materials, raising the likelihood of attacks on infrastructure and other targets. Additionally, the possibility of accidents remains. Emerging and disruptive technologies present both opportunities and challenges for CBRN defence. Hybrid CBRN threats can manifest in several ways. Chemical hybrid threats involve the use of new hard-to-detect chemicals for malicious purposes as seen in the Salisbury poisoning. Biological hybrid threats can erode public trust in science and health systems, exemplified by the dis- and misinformation during the COVID-19 pandemic. Radiological hybrid threats might include cyber-attacks on critical infrastructure, potentially serving as a cover for stealing radiological material for a dirty bomb. Finally, nuclear hybrid threats could involve the sabotage of nuclear facilities or exploiting fears surrounding nuclear incidents, such as those associated with the Zaporizhzhia power plant.**

**Russia has been on the forefront of using hybrid threats, particularly when it comes to disinformation campaigns. China modernises its capabilities and influences its reputation through favourable disinformation. Iran and North Korea target countries through their cyber capabilities and enhance their capabilities respectively.**

**An analysis of the six strategic enablers outlined in NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy (2022) indicates important steps to ameliorate current defences and prepare NATO and its member states for future hybrid CBRN threats, thereby increasing overall resilience. They include important aspects: robust intelligence-sharing mechanisms to ensure timely and accurate threat information; comprehensive exercises to simulate and prepare for various CBRN scenarios; strong partnerships both within the alliance and with external entities to foster cooperation and resource sharing; effective strategic communication to manage information and public perception; collaborative scientific research to advance technological capabilities and countermeasures; and the resilience of medical infrastructure to ensure a rapid and effective response to CBRN incidents. These steps collectively aim to bolster NATO's preparedness and adaptability in the face of evolving hybrid CBRN threats.**

# Contents

# 1. Introduction

In contemporary discourses about war and conflicts, the terms hybrid warfare and hybrid threats are often mentioned. The new threat environment, according to the North Atlantic Treaty Organization (NATO), depicts a variety of threats and threat multipliers, among these so-called hybrid threats (NATO/OTAN, 2022a). This study investigates hybrid threats in the environment of Chemical, Biological, Radiological, and Nuclear (CBRN) defence. It discusses hybrid threats in relation to CBRN defence and identifies present and future challenges. Hybrid threats blend military, and non-military means to undermine an opponent, causing destabilising effects. Hybrid threats are difficult to attribute yet executed with intent, targeting societies to create confusion, disrupt decision-making, and sway public opinion. When combined with CBRN threats, they can significantly magnify the impact or hinder the response to such incidents. Notably, two main considerations surround cyber-attacks and disinformation and their respective impact on the CBRN environment and its defence. This paper aims to contribute to the development of a comprehensive approach in countering hybrid threats, assessing preparedness, and enhancing CBRN defence. This study was composed as part of a research internship by Paulina Frederike Gogacz at the Joint CBRN Defence Centre of Excellence (JCBRN Defence CoE) in Vyškov, Czech Republic, between March and June 2024.

# 2. Methodology, Scope, Limitations

The study is mostly based on literature review and evaluation of publicly available sources. These also include primary source analysis of NATO and EU doctrines, policies, and concepts. The sources were almost exclusively found through internet research and include official reports, briefings, scientific studies, and articles. Furthermore, it includes thoughts and ideas from experts in the field that were collected throughout a series of discussions and interviews at the JCBRN Defence Centre of Excellence.

The general research question of the study is: "**What needs to be considered about hybrid threats in the CBRN environment to be prepared, remain resilient, and defendable as Western democracies?"** The research focuses on two major parts: illustrating hybrid threats in the CBRN environment and highlighting consequential implications and necessities for CBRN defence. The first part analyses the current situation of hybrid threats in the CBRN environment. Initially, the terms hybrid threats and hybrid warfare are explained to establish a common understanding. The paper does not aim to develop a universal definition, it aims to facilitate discussions surrounding these terms by investigating the emergence of the terms in the early 2000s and emphasising the different definitions available. Afterwards, the relationship between hybrid and CBRN threats in strategic-level documents is depicted. Therein, documents from NATO and the European Union (EU) are examined to determine the similarities and differences in the judgement of hybrid threats in the CBRN environment to clarify the current policy perception of the issue. The chapter is followed by a brief depiction of the CBRN environment to comprehend the setting and to identify areas where hybrid and CBRN threats intersect. It draws attention to vulnerabilities in CBRN defence that can be exploited by hybrid threat activities. Examples of hybrid threats in the CBRN environment are given, illustrating the relevance of the issue. The next chapter shows Russia, China, Iran, and North Korea's hybrid and CBRN capabilities. The second part of the study focuses on the strategic enablers outlined in NATO's CBRN Defence Policy. By addressing preparedness and defence necessities through these strategic enablers, the paper highlights considerations for the CBRN environment regarding hybrid threats in a comprehensive approach. Namely, these enablers are shared understanding, capacity-building, partnerships and outreach, strategic communication, scientific and technical collaboration, and medical support.

There are limitations to the research. First, the author of the paper does not have access to classified information. Most of the information used in the paper is derived from open-source material. Moreover,

the interviewees knew that the author does not have security clearance, hence, they did not include classified information during the interviews and discussions. Moreover, the research primarily addresses hybrid threats utilised "below the threshold of war," emphasising the importance and impact of activities within the grey zone. Additionally, due to time constraints inherent in a four-month research internship, the project's scope was limited. The complexity of the topic necessitated focusing efforts within these boundaries. Nonetheless, the arguments presented are robust and offer valuable insights into hybrid CBRN threats.

# 3. Hybrid Threats and Hybrid Warfare

*Therefore, just as water retains no constant shape, so in warfare there are no constant conditions. He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called heaven-born captain.* – Sun Tzu, *The Art of War* (Tzu, 2004, p. 59).

## 3.1. Emergence of „Hybrid“

In the early 2000s, practitioners and academics were looking for a way to conceptualise the seemingly new approach to war. Following the dissolution of the Soviet Union, Europe and NATO flourished and grew as entities. According to scholars, these developments enhanced the asymmetry of power in the international environment (Galeotti, Globsec, 2021, p. 2; Crowther, 2021, p. 21). Coupled with the demonstration of military might during the 1990s conflicts, like the first Gulf War (1990-1991) and the war in Kosovo (1998-1999), the extent of Western power became evident. Consequently, adversaries were looking for different ways to undermine the militarily stronger opponent. (Nilsson, Weissmann, Palmertz, Thunholm, & Häggström, 2021, p. 3; Hicks, et al., 2019, p. 2; Johnson, Russia's Approach to Conflict: Implications for NATO's Deterrence and Defence, 2015, p. 140). In addition, the threat posed by nuclear weapons was neither forgotten nor obsolete, thus, implications of risking escalation were still present (Rühle, 2021, p. 64). The *Center for Strategic & International Studies* (CSIS) attributed the need of adversaries to remain in the grey zone to the U.S. military’s combat edge in high-end warfare and its unwavering nuclear deterrence (CSIS, 2021). These factors shaped the security environment of the 21st century and resulted in adversaries using different tools and activities to inflict harm on the opponent without triggering a conventional war. To describe and discuss this development in warfare, a multitude of terminology exists. Apart from hybrid warfare, often-used terms are also “asymmetrical warfare”, “ambiguous warfare”, or “full spectrum conflict” to name just a few (Nilsson, Weissmann, Palmertz, Thunholm, & Häggström, 2021, p. 2). Thus, from the discourse of the early 2000s, many words emerged to analyse the contemporary circumstances of war and warfare during which adversaries used a combination of means to undermine the opponent, trying to avoid direct confrontation.

Hybrid warfare and later also hybrid threats evolved into stable, but not uncontested, references for these changes in contemporary discussions on the new threat landscape. In 2005, the term hybrid warfare was first used by Frank Hoffmann and Lt. Gen, James Mattis while discussing the war in Iraq, particularly in regard to non-state actors’ accelerated use of irregular methods throughout the conflict (Tenenbaum, 2015, pp. 95-96). Furthermore, Doctor Erin Simpson published a paper with the title “Thinking about Modern Conflict: Hybrid Wars, Strategy and War Aim” the same year (Simpson, 2005). With the 2006 Israeli-Hezbollah war, the term gained notoriety, once again to describe the actions of a non-state actor (Tenenbaum, 2015, p. 96). Therefore, hybrid warfare was originally used to explain and analyse confrontations with non-state actors. The second term, hybrid threats, appeared around 2010, among others in the NATO Capstone Concept (Lasconjarias & Larsen, Introduction: A New Way of Warfare, 2015, p. 5). Synonymous for hybrid threats is also the term “gray zone activities” (Dalton, et al., August 2019, p. 41). At the latest, following Russia’s annexation of Crimea in 2014 and the NATO Wales Summit the same year, both terms became anchored in contemporary rhetoric (NATO/OTAN, 2014). The terms have evolved throughout the past years and no longer are limited to non-state actors’ actions.

Even though the term hybrid sounds like it indicates something new, the idea behind hybrid and the use of unconventional means or combination of different means is not. As mentioned above, the term(s) are not uncontested. Many scholars and critics are quick to point out that using irregular means to damage the adversary has been around for a long time, arguably as long as war itself (Lasconjarias & Larsen, Introduction: A New Way of Warfare, 2015, p. 5; Giles, 2015, p. 321). For example, using non-military actions and other tactics to weaken the adversary was already promoted by Sun Tzu. The Chinese strategist spoke of the importance of the “art of deception” in the sixth century BC. Furthermore, General Joseph Votel describes the Cold War as a 45-year long grey zone struggle which, as mentioned above, is de facto synonymous with hybrid (CSIS, 2021). Therefore, it is obvious that the changed approach to war is not new in the “never-existed-before” sense. However, some aspects have developed. As NATO points out, “the speed, scale and intensity of hybrid threats have increased” (NATO/OTAN, 2024a). Due to technological progress, globalisation, and the digital environment, there are new vulnerabilities to be targeted, particularly in democratic states, as well as enhanced and easily accessible ways to do so (Giannopoulos, Smith, & Theocharidou, 2021, p. 11). Further, the mixed use of activities, through conventional and non-military means, has challenged the Western binary approach to peace and war, and opened discussions about the grey zone environment and how to deal with it (Nilsson, Weissmann, Palmertz, Thunholm, & Häggström, 2021, p. 1). Thus, what is new is that there is an altered and accelerated intensity of the threat.

The critique of both terms does not end with the matter of novelty. Critics often fault the width of the terms, their applications and meaning in strategy and policy. Cox, Bruscino and Ryan argue that hybrid threats should not be understood in a strategic manner but as tactics, because in the strategic context its applicability it is “confusing, incoherent and ubiquitous” (Cox, Bruscino, & Ryan, 2012, p. 28). Elie Tenenbaum also argues that hybrid warfare is “an originally sound concept whose meaning has been diluted to the point of absurdity” (Tenenbaum, 2015, p. 95). The debate on the meaning and suitability of the terms is extensive. That’s why in the following section, the author of this paper tries to clarify the terms in the context in which they will be applied in this study.

## 3.2. Definitions and Characteristics

Hybrid warfare and hybrid threats are not interchangeable; they have slightly different meanings. Hybrid warfare refers to a conflict which has surpassed the threshold of war and consequently no longer takes place in the grey zone. Hence, it refers to an armed conflict according to international law (Łubiński, 2022, p. 5). It's helpful to think of hybrid warfare as the evolving nature of armed conflicts between violent adversaries who use combinations of capabilities to obtain an "asymmetric advantage." (Monaghan, 2019, p. 85). Thereby, they particularly target the military and the effectiveness of its operations (Monaghan, 2019, p. 87). According to Giannopoulos et al. “hybrid warfare represents the hard end of the escalation spectrum of hybrid threats” (Giannopoulos, Smith, & Theocharidou, 2021, p. 41). Thus, hybrid warfare is warfare during which hybrid means or threats are applied.

On the other hand, hybrid threats are employed prior to the escalation into warfare. They can be used to gain advantages and exploit the vulnerabilities of the adversary as part of a strategy, thus remaining in the grey zone (Monaghan, 2019, pp. 86-87). Whereas hybrid warfare targets the military, hybrid threats target the people, society, and the government (Monaghan, 2019, p. 87). Once the threshold of war is surpassed, hybrid threats are referred to in the context of hybrid warfare.

There is no universally agreed-upon definition of hybrid threats. Like terrorism, there are many different definitions circulating in the military, academic and political realm. In the latter, e.g. hybrid threats refer mostly to any “unacceptable foreign interference in sovereign states’ internal affairs” (Giannopoulos, Smith, & Theocharidou, 2021, p. 9). The *Hybrid Centre of Excellence* in Helsinki, Finland, dedicated to the study of hybrid threats, defines them as “actions conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means” (Hybrid CoE, 2024). According to NATO, “hybrid threats combine military and non-military as well as covert and overt means, (…) are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations” (NATO/OTAN, 2024a). These definitions provide orientation for thinking about hybrid threats.

One outstanding commonality is the matter of ill intent. Hybrid activities are used to exploit vulnerabilities. They aim to weaken the targets by undermining or damaging systems, ultimately confusing decision-making, or polarising society (Hybrid CoE, 2019). Mark Galeotti refers to them as "equalizers of asymmetry," as these actions allow the inferior adversary to successfully attack and weaken (militarily) superior actors (Galeotti, Globsec, 2021). *The Landscape of Hybrid Threats: A Conceptual Model* (2021) characterises hybrid threats "force multipliers and/or coercion tactics" (Giannopoulos, Smith, & Theocharidou, 2021, p. 10). Generally, hybrid threats are non-attributable (covert), coordinated with an overarching strategic goal, synchronized with other actions, deliberately conducted with ill intentions, harmful though possibly at first not perceived as such, and multidimensional (Weissmann, 2021; Galeotti, Globsec, 2021; Hybrid CoE, 2019; Hicks, et al., 2019, pp. 3-4). These characteristics and the aim to damage without being recognised as the source of the attack make them effective, yet difficult to counter.

The tools used are ever-changing and ever evolving. Some examples include creating and exploiting infrastructure or economic dependencies, airspace violations, promoting social unrest, creating confusion or contradictory narratives, disinformation campaigns and many more (Giannopoulos, Smith, & Theocharidou, 2021, pp. 33-35). Another tool used by Russia is the weaponisation of migration at Polish and Latvian borders (Łubiński, 2022, p. 2). Problematic is also that the danger posed by hybrid threats is not always visible at first. Sometimes the extent of the impact is only revealed later and at that point it might be difficult to divert an escalation as the opponent has successfully realised its strategy that was guiding the hybrid attacks.

To sum up this chapter, the terms hybrid warfare and hybrid threats emerged in the beginning of the 2000s, originally describing the new ways non-state actors posed an accelerated problem as they used a combination of military and non-military means to undermine the militarily stronger opponent. Whereas hybrid warfare refers to the conduct of war that includes the application of hybrid techniques, hybrid threats are actions that take place outside the theatre of war. They have destabilising effects, are difficult to attribute, yet are conducted intentionally. They target the society and aim to confuse, impair, and influence decision-making and public opinion. This paper spotlights these hybrid threats in the CBRN environment to highlight the intertwinement of the two threats in the present and future security environment.

# 4. Relationship between Hybrid and CBRN threats in Strategic Documents

When hybrid threats were first discussed in the CBRN environment, there was a focus on CBRN materials being (mis)used by non-state actors. In the meantime, countering hybrid threats has become a key component of NATO-EU cooperation as outlined in the 2016 Warsaw Joint Declaration (Tusk, Donald; Juncker, Jean-Claude; Stoltenberg, Jens, 2017). This chapter of the paper looks at the relationship between hybrid and CBRN threats described in contemporary NATO and EU strategic documents to derive similarities and differences).

## 4.1. Strategic Level NATO Documents

For establishing the relationship between hybrid and CBRN threats in strategic level NATO documents the following four documents were analysed: NATO's *2022 Strategic Concept* (NATO/OTAN, 2022a), NATO's *Countering hybrid threats* (NATO/OTAN, 2024a), the *NATO 2030: United for a New Era Report* (Reflection Group appointed by the NATO Secretary General, 2020), and most importantly the NATO's *Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy* (NATO/OTAN, 2022b). The NATO CBRN Defence Policy mentions a "nexus of hybrid and CBRN threats" (NATO/OTAN, 2022b). An obvious similarity between hybrid and CBRN threats is that the pool of adversaries is the same. This is

related to the overall security environment that consists of these actors. Regarding the "nexus," there are two main ways of interconnection between the two kinds of threats described.

The first option is that hybrid threats are utilised in a manner that complicates or hinders an adequate response to CBRN incidents (NATO/OTAN, 2022b). One example is the 2018 poisoning of Sergei Skripal, during which Russian disinformation made the initial response to the attack with the nerve agent Novichok on British soil more difficult and confused.The second possibility is that CBRN materials can be used as tools in hybrid threat activities. This includes new means of delivery for CBRN materials or new CBRN materials that fall under the threshold of current detection mechanisms and techniques (NATO/OTAN, 2022b). The use of CBRN materials is associated with a high potential for fear, which can be exploited by hybrid threats like disinformation and have destabilising consequences.

When it comes to countering these threats or the combination thereof, the approaches foreseen by NATO are remarkably similar. Generally, being able to defend and respond to both threats, hybrid and CBRN, is the responsibility of the nation state. NATO merely plays a supporting role in the processes (NATO/OTAN, 2022b) (NATO/OTAN, 2024a). That's why NATO's role is to define requirements for nations to be able respond to these threats. For both, the two main necessities are to increase the countries and alliance's resilience as well as the defence capabilities for which training, education and exercise are crucial (NATO/OTAN, 2024a) (NATO/OTAN, 2022b). Moreover, civil-military cooperation is underlined in both, as it is vital "to ensure military readiness and national resilience" (NATO/OTAN, 2022b). The CBRN Defence Policy summarises six so-called strategic enablers that enhance resilience and defence capabilities.

Regarding resilience, the CBRN Defence Policy mentions the seven baseline requirements, established by the alliance during the 2016 Warsaw Summit. Every NATO country is required to be able to sustain these demands during times of crises which could, inter alia, be a hybrid and/or CBRN attack. The requirements are the following:

- "Continued governmental services,
- Resilient energy supplies,
- Containment of uncontrollable mass movement,
- Resilient food and water supplies,
- Dealing with mass casualties,
- Resilient communication systems,
- Resilient transportation systems."

Furthermore, NATO is working on "*Layered Resilience*",[1] as part of the five warfare development imperatives, that can be used as the foundation for the resilience for both CBRN and hybrid threats. One crucial aspect about resilience, particularly regarding hybrid threats, is the necessity of identifying one's own vulnerabilities (NATO/OTAN, 2024a). Hereby the 2022 Strategic Concept underlines the importance of retaining military interoperability and military edge by investing and updating emerging and disruptive technologies (NATO/OTAN, 2022a, p. 7). Further, NATO has set out non-binding guidelines for civil preparedness in the event of a CBRN incident that countries can use as orientation and to accelerate their resilience, regarding planning, logistics, medical support, public awareness and warning information systems, notification and emerging communications, and training and exercises (Defence Policy and Planning Division, 2019).

Defence capabilities refer to the abilities to "counter malign interference, prevent destabilisation and counter aggression" (NATO/OTAN, 2022b). Both threats or the combination thereof have demanded NATO's attention and during the past years, NATO formed support teams to reinforce the defence against each of these threats. For hybrid threats it is, among other, the *Counter Hybrid Support Teams*

[1] Layered resilience refers to the project that entails many, mutually reinforcing parts to resilience in the military and in the civil sector that help to resist and manage problems and out-last attacks. It is an on-going NATO project, aiming to be finished in 2025. It consists of many work strands, one of which is the concept of layered resilience comprehensive of seven thematic working groups one different areas of military resilience (C2 System, Situational Awareness, Warfighting Capabilities, Logistics, Response Planning, Perseverance, and Military Infrastructure) It is supposed to give the countries a roadmap to understand the importance of it.

which were formed in 2018 as well as the hybrid analysis branch of the *NATO Joint Intelligence Division* which was created in 2017. The former offer support upon request to respond to hybrid threats, while the latter is supposed to accelerate situation awareness, with a particular focus on hybrid activity (NATO/OTAN, 2024a). With all of these steps, NATO enhances its toolbox for dealing with hybrid threats which is continuously updated to have a better understanding of the changing hybrid threat environment. In addition to the national CBRN troops, NATO also developed, among others, the *Combined Joint CBRN Defence Task Force*, a response body to CBRN incidents, and the *CBRN Reachback Element*, which is responsible for scientific, technical, and operational CBRN assessments and advice. Then there is also the *Joint CBRN Defence Capability Development Group*, responsible for developing new capabilities and updating doctrine in CBRN defence, allowing the Alliance to be on track with the evolving CBRN defence environment.

## 4.2. Strategic Level EU Documents

Having looked at the relationship between CBRN and hybrid threats in strategic-level NATO documents, the next step is to do the same for the EU. The three main documents used are the 2016 *Joint Framework on countering hybrid threats*, (European Commission, 2016), the 2017 *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*, (European Commission, 2017) and the 2018 *Increasing resilience and bolstering capabilities to address hybrid threats* (European Commission, 2018). The 2022 EU strategic compass was also analysed. However, whereas hybrid threats are a reoccurring danger discussed, CBRN threats are not even mentioned once (European External Action Service, 2022). There are only general discussions about critical infrastructure, proliferation of weapons of mass destruction, and crisis management that hint in the direction of CBRN. Moreover, the 2024 progress report only mentions CBRN in relation to emergency assistance to Ukraine (European Union External Action, 2024, p. 10).

On the relationship between the two threats, the document from 2016 does not cover much. Concerning the CBRN-issue, it mentions the possibility of bioterrorism. Additionally, the document specifically looks at the possibility of manipulation of diseases and contamination of food, soil, air, and water with CBRN agents (European Commission, 2016, p. 9). For these cases, crisis communication guidelines and simulations for training need to be put forward to build capacity and strengthen health security, environmental protection, and food safety. Lastly, it is mentioned that member states can use the *Common Security and Defence Policy* (CSDP), inter alia, for “help in specialised areas such as CBRN risk mitigation (…)” (European Commission, 2016, p. 16). Thus, in the document the possibility of CBRN incidents in the realm of hybrid threats is acknowledged, yet to a limited degree.

The 2018 document combines the two areas and sets out the relationship between the threats in the EU’s understanding. It is important to mention that the document was published in the aftermath of the 2018 Skripal poisoning scandal. Three noteworthy claims are made about the relationship between hybrid threats and CBRN incidents. First, the Novichok incident in Salisbury “underlined the versatility of hybrid threats and the multitude of tactics now available” (European Commission, 2018, p. 1). It identifies the incident as a part of hybrid campaign. Secondly, it is pointed out that “threats posed by non-conventional weapons fall in a category of their own (…)” (European Commission, 2018, p. 1). This is due to the level of damage possible related to the materials. According to the EU, despite CBRN incidents being an indicator of how diverse hybrid campaigns have become, CBRN attacks make up a separate category. This claim is reaffirmed in the last point. CBRN threats can share many characteristics of hybrid threats (“difficult to detect and attribute”) but they go further and are “a general concern for the international community” (European Commission, 2018, p. 1). As such, the category of CBRN threats needs to be considered separately in detail due to the risks associated with the use of CBRN material.

Countering hybrid threats and CBRN threats is outlined respectively in the 2016 *Joint Framework* and the 2017 *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*. The 2016 framework sets out 22 items to implement for countering hybrid threats. It identifies hybrid threat defence as ultimately the member countries’ responsibility as vulnerabilities are individual (European Commission, 2016, p. 2). The actions aim for “improving awareness, building resilience, preventing, responding to crisis and recovering” (European Commission, 2016, p. 3). There are different subchapters. The most relevant cover intelligence (the formation of the hybrid fusion cell

within the *EU Intelligence and Situation Centre*), STRATCOM, resilience in key infrastructures, supply chains and society, cybersecurity capabilities for industry, energy, financial systems and transport systems and prevention of radicalisation. In 2017, the EU set out 23 actions that need to be taken to advance "prevention, preparedness and response" of/for/to CBRN incidents (European Commission, 2017, p. 3). All of them are guided by the four main objectives, which include reduced access of CBRN materials, preparedness for and ensured response to incidents, internal-external links with regional and international partners, and enhanced knowledge on CBRN risks (European Commission, 2017, p. 4).

The 2017 action plan for CBRN is mainly set out against the backdrop of non-state actors and particularly terrorist organisations using CBRN materials (European Commission, 2017, p. 2). Implementation of the above-mentioned four objectives is supposed to be done in a cross-sectorial and multi-faceted manner. Different organisations must cooperate and coordinate their work to achieve security. The formation of hubs and expert groups is one way to achieve it. As there is such a focus on possible terrorist groups using CBRN, the *European Counter-Terrorism Centre* (ECTC) set up a dedicated CBRN knowledge hub within the organisation (European Commission, 2017, p. 13). Furthermore, Europol was also required to develop a CBRN knowledge hub. (European Commission, 2017, p. 14) For CBRN-related preparations, the *CBRN Advisory Group* was formed and is responsible for examining and analysing detection equipment and keeping CBRN defence up to date. Operationally, this group is supported by the so-called *EU CBRN Support Network* of CBRN centres and networks for expertise (European Commission, 2017, p. 13). Lastly, cooperation with NATO (on information exchange, capacity-building, training, and exercise) and other specialised organisations like the IAEA, Interpol, and the OPCW are underlined (European Commission, 2017, p. 12).

In 2021, the European Parliament released a study on *EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats* (Rimpler-Schmid, et al., 2021). It considers gaps in CBRN preparedness and defence and recommends steps to fill the discovered gaps. One of the suggestions for increasing CBRN preparedness is for it to be "linked to hybrid threats and other crosscutting issues that have CBRN dimension" (Rimpler-Schmid, et al., 2021, p. 89). The report points out that looking at CBRN threats from an isolated perspective it not enough, it needs to be looked at from the complex threat environment that involves a multitude interconnected threats, actors, and possibilities.

## 4.3. Similarities and Differences

Comparing the two organisations and their approach to hybrid CBRN threats, some similarities can be identified. Both acknowledge the evolving nature of security threats, including hybrid tactics that combine conventional, irregular, and CBRN elements to achieve strategic objectives. Both documents highlight the need for comprehensive approaches to address hybrid threats effectively. The responsibility to address and counter them lies with the nation states, as these threats correspond to country-specific vulnerabilities and capabilities. However, the effects of hybrid and CBRN threats can exceed national borders and may require a coordinated response. In terms of responding and achieving situational awareness, both underline the importance of intelligence. For intelligence, both organisations have adapted their intelligence institutions, the *NATO Joint Intelligence and Security Division* and *the EU Intelligence and Situation Centre*. Both have dedicated hybrid sections, NATO calling it the *Hybrid Analysis Branch* and the EU referring to it as the *Hybrid Fusion Cell*. Both NATO and the EU emphasise the importance of building resilience to hybrid threats, including in the CBRN environment. They recognise the need for enhancing preparedness, response capabilities, and societal resilience to mitigate the impact of hybrid tactics, including CBRN-related incidents. Points like strategic communication and disinformation, safeguarding key infrastructure, and cybersecurity are highlighted by both. Lastly, both documents advocate for a multidimensional approach to addressing hybrid threats, encompassing military, civilian, and societal dimensions. They emphasise the importance of cooperation and coordination among various stakeholders, including government agencies, international organisations, and the private sector, to counter hybrid threats effectively.

Nevertheless, differences can also be found. The NATO CBRN Defence Policy primarily focuses on enhancing the capabilities and readiness of the military alliance to respond to CBRN threats, including hybrid tactics. In contrast, the EU emphasises the importance of civilian cooperation and resilience-building measures, with a focus on strengthening critical infrastructure, public services, and societal

resilience. This underlines the different nature of these international organisations. While both NATO and the EU stress the importance of cooperation, their approaches differ in scope. NATO's cooperation primarily involves member states and partner countries within the alliance framework, with a focus on military interoperability and information-sharing mechanisms. The EU's cooperation extends beyond its member states to include neighbouring countries and international partners, with a focus on capacity-building, technical assistance, and knowledge exchange to enhance resilience against hybrid threats. The NATO CBRN defence policy integrates hybrid threats into its broader framework for addressing CBRN incidents and emergencies. In contrast, the EU addresses hybrid threats as part of a broader strategy for increasing resilience and bolstering capabilities across various sectors, including energy, transport, and healthcare, with specific reference to the potential intersection with CBRN threats. Another difference concerns the connection between hybrid and CBRN threats. In 2021, the EU identified the gap of not focusing enough on the interconnectedness of threats. NATO has already acknowledged it in their CBRN Defence Policy by specifying it and talking about a “nexus.” The threats do not only pose a challenge as separate issues but the combination of the two is an even further-reaching hazard. Thus, while both the NATO and the EU recognise the importance of addressing hybrid threats in the CBRN environment, they differ in their focus, scope of cooperation, and integration of hybrid threats into their respective CBRN frameworks for enhancing resilience and bolstering capabilities.

# 5. CBRN Environment

Cases in the CBRN environment range from accidents to highly consequential attacks. When talking about CBRN defence, NATO means the non-proliferation of weapons of mass destruction (WMDs), defence against CBRN incidents and attacks, and the capability to recover from such events (NATO/OTAN, 2022b). According to NATO, “any chemical, biological, radiological, or nuclear substance that may pose a hazard to NATO populations, territories and forces, regardless of origin or whether the material was originally conceived as a weapon” is considered CBRN material (NATO/OTAN, 2022b). Incidents involving these sorts of materials easily create panic. In the 1995 Tokyo subway attack, 54 people were critically injured, yet almost 6000 uninjured people also requested medical assistance out of fear of contamination (Bennett, et al., 2022, p. 15). This example shows that the CBRN environment encompasses a large, detrimental, and sensitive area of security.

Similarly to the underlying concepts of hybrid threats, the use of CBRN materials is also ancient. Consequently, the issue of trying to regulate the threat level is also not new. After World War I, in 1925, there was an attempt to ban biological weapons with the Geneva Protocol (Dupuy & Viñuales, 2018, p. 429). The employment of biological weapons was further curtailed about fifty years later. The 1972 *Convention on Biological Weapons* did not solely ban the use of these weapons but also banned other aspects of the life cycle of these weapons, like development, production and stockpiling of them as well as providing them to terrorists (Dupuy & Viñuales, 2018, p. 430). The *Chemical Weapons Convention* was ratified in 1993. It covers jus in bello (guidelines for conduct in armed conflicts) as well as non-proliferation aspects. With the *Organization for the Prohibition of Chemical Weapons* (OPCW), the implementation of the convention is better enforced than the one for biological weapons (Dupuy & Viñuales, 2018). But as examples in Syria show, chemical weapons are still being used in armed conflicts which raises questions about the effectiveness of either convention. Regarding nuclear weapons, universal agreements on bans do not exist. The closest agreement is the *Treaty on the Non-Proliferation of Nuclear Weapons* which has been valid since 1970. It aims to stop the dissemination of nuclear weapons. One major reason for the difficulty is that nuclear states block total bans, as examples like the July 2017 *Treaty on the Prohibition of Nuclear Weapons* show which was signed by 93 parties but major nuclear states like the U.S., Russia, or China are not among the signatories (United Nations Office for Disarmament Affairs Treaties Database). As it can be derived from this part, legal regulations of CBRN materials have only limited success when it comes to the prohibition of these weapons.

Apart from attacks including CBRN materials, technical failures at chemical or nuclear power plants, leaks from biological laboratories or theft of radiological material from hospitals are also possible CBRN threats. Being aware of the large range of threats, going beyond the sensationalised attack is necessary for a well-rounded understanding of the environment. Currently, the threat is increasing as the actors using CBRN materials are diversifying and feel less obliged to follow the international rules. The concern of state actors using them in conflicts is growing, as more countries are willingly breaching commitments enshrined in international treaties. Non-nuclear countries are enhancing their nuclear capabilities, nerve agents are used for political assassinations and chemical weapons have been used in the Syrian War. (Schmitt, 2016) Non-state actors benefit from technological developments which facilitate the access and dissemination of CBRN materials.There are many emerging and disruptive technologies that demonstrate the ability to innovate and evolve the CBRN threat. With dual-use technologies, the issue is that they can be used for both peaceful and disruptive purposes. In the CBRN environment, not only do the materials themselves fall into the dual use category but also the technologies surrounding them do and that's why supervision can become a guessing-game. Uncrewed aerial vehicles (UAVs) redefined means of delivery of CBRN agents. Drones are cheap, small, easy to control and can even be built with a few components. Drones fall into the category of dual use because they are employed in the civilian sector for landscape photography and agricultural uses, but they have also shown to be useful in more recent wars, such as the ongoing war in Ukraine or the 2020 Nagorno-Karabakh conflict.[2] (Franke, 2023)

Furthermore, accessing weapons is facilitated through technologies like 3D printing. Weapons, parts of UAVs, and even miniature missiles can be built at home with the technology of 3D printing. In a 2019 terror attack in Germany, the perpetrator Stephan Balliet used weapons that he created in a 3D printer. In October 2019, Balliet livestreamed his attempt to forcefully enter a Synagogue in Halle, Germany. He failed in this attempt; however, he shot two victims (Koehler, 2019, p. 14). It was allegedly the first time that a terrorist attack included homemade weapons that included 3D-printed components. This event "crossed a new threshold in weapons improvisation in terrorism" which even overcame detection mechanisms in place to spot high-risk individuals (Koehler, 2019, p. 18).

Lastly, artificial intelligence technology revolutionises technology in every sector, also in CBRN. Advanced algorithms and AI can be used to, among other things, autonomously drive cars, drones, even ships and can even create new molecules. AI can also alter the accuracy of targeting systems and, consequently, is central to discussions regarding nuclear weapons systems (Prof Puwal, 2024). The threats are diversifying and progressing, but it needs to be said that the level of progress is also enabling better defence capabilities to counter these new advancements. This paper will dive deeper into this subject in the second part, particularly in the chapter focusing on scientific and technical collaboration. The next part will look at the different components of the CBRN environment and illustrate the different threats, also regarding hybrid threat activities.

## 5.1. Chemical Threats

Chemical-warfare agents can be classified in four main categories, namely nerve agents, choking agents, blood agents, and blistering agents (Madsen, 2023). All these toxic agents cause serious harm or death in contrast to riot-controlling agents which only cause temporary discomfort. With chemical weapons, sometimes, the combination of two harmless chemicals can create deathly outcomes. One example is the assassination of Kim Jong-Un's brother who was killed at the Malaysia airport with the nerve agent VX in 2017 (Ellis-Petersen, Lumpur, & Haas, 2019). In his case, two different chemicals were smeared on his face and the reaction thereof created VX and killed him.

Apart from having chemicals that in their combination have lethal effects, there is the issue of chemicals that are hard to detect. Some new and old chemical agents can fall into this category and consequently can be considered hybrid CBRN threats. There are many examples. The use of chlorine in Iraq, the use of mustard gas by ISIS and the use of chemicals by Russia in the ongoing War in Ukraine (Schmitt, 2016; Badshah, 2024). In recent years, there have been incidents of hard-to-detect chemicals being used, even on foreign soil, for political assassinations. They have been used in a manner to demonstrate power and spread fear in populations and impair decision-making, which makes them a hybrid threat.

[2] Interview 3,4

Admittedly, attribution might be difficult yet not impossible. One example is the poisoning of former Russian spy Skripal and his daughter Yulia in Salisbury, England. The so-called A-agent chemicals (like Novichok which was used in this case) were designed to be undetected by NATO chemical detection equipment and circumvent detection and CWC guidelines (Noga & Jurowski, 2023).

### 5.1.1. Skripal/Salisbury poisoning

In March 2018 Sergei Skripal and his daughter Yulia Skripal were found almost unconscious with foam coming out of their mouths on a bench in the English town of Salisbury (Schwirtz & Barry, 2018). Both were saved in the hospitals and survived the incident. Skripal was a former GRU [3]spy who had lived in Salisbury England since the spy exchange in 2010, where he was released to the West, after having been imprisoned in Russia for providing secret information to foreign intelligence services (Schwirtz & Barry, 2018). Inquiries and investigations concluded that the Skripals were poisoned with the nerve agent Novichok that was spread on their door handle (Schwirtz & Barry, 2018). The nerve agent was transported through a perfume bottle from Russia to the United Kingdom (BBC, 2018). The bottle was later found by Charlie Rowley and his girlfriend Dawn Sturgees, the latter of whom died after applying some of the perfume's content (BBC, 2018). Novichok is a type of chemical that is hard-to-detect and thus it was possible to transport it through airport security.

Novichok is not a new chemical. Despite the name meaning "newbies," the Soviet Union started its research in the 1970s. (Boland & US, 2018). They were designed to be undetected by chemical detection equipment used within NATO countries (Boland & US, 2018). Being a nerve agent, Novichok binds to the enzyme acetylcholinesterase and inhibits the breakdown of the neurotransmitter acetylcholine, causing constant signal transmission between synapses and, consequently, disturbing the nervous system (Noga & Jurowski, 2023). In recent years, Novichok has been related to a few cases of Russian-backed poisonings. These toxic agents were also used for the poisoning of Navalny in 2020 (Tagesschau, 2020). These incidents aimed to raise fear in Russia's opposition and former agents. Russia denies accusations but investigations have proven the sources of these attacks.

In the case of the Skripal poisoning, the independent investigative website *Bellingcat* was able to reveal the true personalities behind the perpetrators. Through extensive open-source research they exposed the two men behind the aliases Ruslan Boshirov and Alexander Petrov as Anatoliy Chepiga and Alexander Mishkin, two GRU officers (Higgins, 2021). Russia tried to cover up the incident through establishing counter-narratives. "Ruslan Boshirov" and "Alexander Petrov" appeared on *Russia Today*, claiming in an interview with Margarita Simonyan to have visited Salisbury as tourists, wanting to see infamous cathedral (Harding, 2020). As the interview was not convincing, the Russian envoy to London Alexander Yakovenko insisted that Bellingcat is part of the "deep establishment" and as such cannot be trusted, another attempt to distract from the findings (Harding, 2020). Russia's influence attempts on distorting the truth despite available proof demonstrates the commitment to pushing disinformation to erode trust and spread confusion surrounding a CBRN incident.

The case of the Skripal poisoning discloses two difficulties regarding hybrid CBRN threats. First, the chemical Novichok is hard to detect and falls into the category of CBRN materials being used alongside hybrid activities. Secondly, the investigation into the incident was hindered as Russia kept on denying claims and spreading further narratives to confuse the conversation. In the case of the Skripal poisoning, the disinformation attempts were not very successful, nevertheless, it highlighted the current era of truth-decay. The British government answered quickly, but ultimately, they benefited from Bellingcat's investigation.

## 5.2. Biological Threats

Like chemical threats, biological threats comprehend a large and advancing field. New technologies create new possibilities which can be used for scientific progress in different fields like medicine or have a highly destructive potential as weapons. Bioweapons and biological materials have been used in the past for offensive purposes. During the two world wars, countries like Germany, Japan, the U.S. and Britain developed biological warfare programmes (Oliveira, Mason-Buck, Ballard, Branicki, & Amorim,

[3] GRU is Russia's military intelligence service (the acronym is still from the Soviet times when it was called Main Intelligence Directorate - Гла́вное разве́дывательное управле́ние)

2020, p. 3). Incidents of non-state actors having access to such material can be demonstrated in examples like the anthrax letters in 2001 or the attempts by Al Qaeda and ISIS to obtain these weapons (Headley, 2020; FBI).

Emerging technologies like AI have an enormous impact on bioengineering and biotechnology. Biological and human enhancements (BHET) allow genetic manipulation that could lead to targeting or the creation/recreation of biological agents. Eleonore Pauwels focuses on AI's influence on biosecurity in the Hybrid CoE's Strategic Analysis / 26 *Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks.* She explains how the switch from analogue to digital turned biosciences into critical information infrastructure. Many processes are conducted "in silico," meaning with synthetic datasets, algorithmics and advanced computing. But with these developments and the digitalised and decentralised mode of bioengineering come major security challenges, as "AI can be misused to manipulate datasets in seconds, creating hybrid insecurity flashpoints and leading to widespread collective data harms, research and industrial sabotage, as well as compromised governance systems and data integrity crucial to health, food and civilian security" (Pauwels, May 2021, p. 3). Thus, emerging technologies like AI play a crucial role in the development of biological threats and the damage cyber-attacks or other sabotage activities can cause.

Another implication of hybrid threats are the consequences of lowering people's trust, particularly concerning science and the health system. Eroding trust affects more areas than the scientific research, but the "damaging impact would be on citizen's trust in governing institutions, emergency data systems, industrial laboratories, food supply chains, hospitals and critical health infrastructure" (Pauwels, May 2021, p. 6). One recent example that depicts the gravity of citizens losing trust in the health care system is the vaccine hesitancy that followed the COVID-19 pandemic. Consequences affected not only the hesitancy toward the COVID-19 vaccination, but also others and resulted in a decline in vital children's immunisation for diseases like measles or polio (WHO, 2022). In the following section, the effects of conspiracy theories and disinformation on eroding trust will be discussed using the COVID-19 pandemic and the purported biological laboratories in Ukraine as examples.

### 5.2.1. COVID-19 and Biolabs in Ukraine: Disinformation and Conspiracy theories

Hybrid threats have destabilising effects and are hard to attribute. The impact of disinformation is a good indicator to depict their effectiveness, e.g. with the accelerating distrust among Western societies. According to the 2024 the World Economic Forum's *Global Risks Report 2024*, mis- and disinformation is the most severe global risk for the next two years, among other influencing discourses on public health (World Economic Forum, 2024, p. 8). The risk is further accelerated as AI is used to generate the content and disseminate it to a wider audience. To clarify some of the terms, whereas misinformation is the "false or inaccurate information spread without malicious intent", disinformation is the "false or inaccurate information spread deliberately to manipulate the opinions and actions of others" (NATO/OTAN, 2023). The deliberate spread of false information has shaped the global security environment for a few years now, and the negative effects are revealing themselves.

Sometimes disinformation in based on existing or new conspiracy theories. Generally, there is a peak visible in the spread of conspiracy theories during crisis events (Basit, 2021, p. 2). As it was said in Chapter 3 that the speed, scale, and intensity of hybrid threats has increased, the same goes for the spread of conspiracy theories in current times. As Basit points out, "social media platforms have also allowed disparate conspiracy groups and movements to form networks and spawn into a global phenomenon" (Basit, 2021, p. 2). Douglas et al. explain that people believe in conspiracy theories, among other, because "they promise to satisfy important psychological motives that can be characterised as epistemic (e.g., the desire for understanding, accuracy, and subjective certainty), existential (e.g., the desire for control and security), and social (e.g., the desire to maintain a positive image of the self or group)" (Douglas, et al., 2019, p. 7). In the CBRN domain the prevalence of conspiracy theories can have detrimental consequences as they erode trust in science and scientific institutions. This is already visible as they have "driven people to reject mainstream medicine to the point where once-cured diseases are now making a comeback in some parts of the world" (Douglas, et al., 2019, p. 4).

Pummerer et al. investigated the consequences of belief in conspiracy theories related to COVID-19 on people's attitudes and behaviour during the pandemic. They concluded that "the confrontation with and the belief in conspiracy theories are associated with less institutional trust and lower support for and adoption of regulations put forward by these institutions" (Pummerer, et al., 2022, p. 56). There were and still are a lot of conspiracies, misinformation and disinformation about the COVID-19 pandemic. Studies have proven that China and Russia deliberately embraced information operations surrounding the COVID-19 pandemic (Dubow, Lucas, & Morris, 2021). According to Dubow, Lucas and Morris, whereas China is mainly focusing on "narrative consistency" and positively portraying its efforts, Russia sticks to the "firehose of falsehoods strategy" to polarise societies abroad, while depicting alleged scientific superiority, meaning that they share a lot of content and narratives, caring more about quantity than quality (Dubow, Lucas, & Morris, 2021). One example is the COVID-19 vaccine. Russia's disinformation thereupon focused on boosting trust in its own vaccine Sputnik V and negatively portraying Western vaccines like Pfizer (Dubow, Lucas, & Morris, 2021). Already during but mostly after the COVID-19 pandemic there was a globally noticeable rise in vaccine hesitancy, not solely for the COVID vaccine but other vaccines as well. Altman et al. argue that vaccine hesitancy could be decreased by minimising misinformation on vaccines (Altman, et al., 2023, p. 4). In their study, many participants have cited social media as a reason for their refusal or hesitancy to receive a COVID-19 vaccine (Altman, et al., 2023, p. 7). Eurofound's study has found out that in Europe the trust in national institutions has decreased by 13.4% between the start of the pandemic and spring 2022. Specifically, regarding the healthcare systems, it has decreased by 10.2% (Eurofound, 2022). This is how misinformation and disinformation can directly impact society and biosecurity.

Another example of how disinformation has shaped discussion around the issue of biosecurity is the deliberate false claim by Russia about biological laboratories in Ukraine prior to the outbreak of the war. Russian state media has spread the theory that the Ukrainian territory hosts U.S.-funded laboratories that conduct research on and produce biological weapons. The biological laboratories were allegedly used to have birds and bats spreading biological weapons or create ethnic bioweapons in the form of enhanced capabilities of Ukrainian soldiers (Parachini, 2022). It is true that the U.S. has financially contributed to biological laboratories in Ukraine since 2005, but not for the reasons claimed by Russia (Qiu, 2022). The narrative also plays into the bigger conspiracy theory that the West is trying to undermine Russia and destroy it, a narrative that has been boasted by Russian information campaigns in recent years to justify malicious actions abroad. The accused laboratories do epidemiological surveillance with neighbouring countries and international partners like the World Health Organization or World Organization for Animal Health (Parachini, 2022). Russia's claims are dangerous, as they undermine the efforts of international arms control agreements. Using these platforms to legitimise disinformation is dangerous and "allowing Vladimir Putin's regime to use this false narrative to distract attention from his imperial invasion could risk setting a precedent that other rogue regimes may follow" (Parachini, 2022). The case demonstrates that some states go to extreme levels to have their narratives accepted as truth. However, in areas like public health, where public trust is important, the consequences of increased disinformation and conspiracy theories are detrimental.

## 5.3. Radiological and Nuclear Threats

Radiological threats, while not as immediately catastrophic as nuclear threats, still pose significant risks to public health, safety, and security. In the radiological domain, threats can arise from different sources. They include the illicit acquisition or theft of radioactive materials, accidents involving radiation-emitting devices or industrial facilities, and deliberate dispersal of radioactive substances as part of terrorist attacks or sabotage operations with the use of "dirty bombs". The "dirty bomb" or radiological dispersal device (RDD) are classic explosives that contain radioactive material, which means that, apart from the dangers posed during the blast, there is also the risk of radiation and contamination. (Council on Foreign Relations, 2006) These threats can result in radiation exposure, contamination of the environment, long-term health effects for affected populations and create panic. (Interpol, 2017) Under the aspect of hybrid tactics, they could focus on exploiting vulnerabilities in radiological security or infrastructure, including cyber attacks targeting radiation monitoring systems or medical facilities using radioactive materials or coordinated physical attacks on transportation routes carrying radioactive sources. Theft of radiological material in transit has been a problem for some time as the IAEA reported that 52% of all thefts of radioactive materials since 1993 and 65% in the past ten years have happened during the transport

(IAEA, 2024). Hybrid CBRN threats can also involve the theft of radiological material using a cyber attack as a cover up. Lastly, disinformation campaigns can be used to create more fear and panic around a radiological hazard, exacerbate the consequences of radiological incidents or complicate response efforts.

In the nuclear domain, threats can emanate from states with established nuclear arsenals, such as Russia, China, the U.S., and others, as well as from state or non-state actors seeking to acquire nuclear capabilities like Iran. Nuclear technology has destructive potential in the form of nuclear weapons and their long-lasting consequences. Additionally, many countries rely on it as an energy source. Hybrid CBRN threats can manifest in various forms, including cyber attacks targeting nuclear facilities' control systems, sabotage operations aimed at disrupting nuclear operations or stealing nuclear materials. Risks of espionage are also heightened with technologies such as uncrewed aerial vehicles (UAVs). Basically, the threat evolves around vulnerabilities in nuclear security, infrastructure and energy security. They can also be disinformation campaigns aimed at undermining public confidence in nuclear safety, energy and security measures. Nuclear energy has been a contested topic for decades. Despite public opinion becoming more supportive in some countries like the U.S (Merrifield, 2024), in other countries scepticism remains high as the example of Germany shows (Thurau, 2024). Lastly, the fear regarding the nuclear threat can be used to manipulate and disrupt decision-making. Countries threatening to use their nuclear arsenal in a conflict raises the stakes and has psychological effects on decision-makers and the public. One example which will be elaborated in the next section is the way in which Russia has been using the fear around the Zaporizhzhia nuclear power plant strategically to influence debates around the conflict in Ukraine.

### 5.3.1. The Stuxnet Affair & The Zaporizhzhia Nuclear Power Plant

Concerning the use of hybrid threats in the nuclear domain two examples will be briefly outlined. The first case focuses on the Stuxnet cyberweapon that was discovered in the early 2010s and depicts the difficulty of detecting malware and its impacts on infrastructure. The second case surrounds Russia's current use of fear regarding the Zaporizhzhia power plant in Ukraine and how the level of insecurity affects decision-making in the West.

Stuxnet is a good example to show how hybrid techniques can have practical influence on developments in CBRN. The Stuxnet malware is often called one of the first cyberweapons. The worm was discovered in 2010 and aimed to delay the Iranian nuclear programme and is consequently the first cyberweapon directly targeting infrastructure (Fildes, 2011). It targeted the uranium enrichment process by attacking Windows and Siemens software and the software on the programmable logic controllers of the centrifuges and changed their speed as a result (Fruhlinger, 2022). Changing the speed affected the enrichment process, meaning that Iran could not effectively enrich the uranium which delayed their nuclear programme. It is officially not clear who created the malware, but the most probable sources are the U.S. and Israel, as the creation of the malware is so complex that it must have been governmentally supported (Kushner, 2024). It has been over a decade since this cyberweapon was detected. In the meantime, cyber capabilities are improving, and especially critical infrastructure is a likely target. But the incident proves that cyber security against espionage is not enough. Cyber security of infrastructure together with hardware and software are also important to safeguard.

The Zaporizhzhia nuclear power plant has been constantly in discussions during the war in Ukraine. Since the beginning of the war, it has been under attack on many occasions, raising fear of nuclear safety and security risks associated with wars in countries with advanced infrastructure (Alkis, 2024). The mere presence of military operations in the vicinity of such a critical infrastructure creates a persistent threat of potential nuclear disaster which can have catastrophic consequences for civilian populations, the environment, and neighbouring countries (United Nations, 2024). Russia's control over the plant and its ability to threaten or imply threats of a nuclear incident have caused disruptions, characteristic for hybrid threats. These actions have disrupted diplomatic efforts and strained alliances, as Ukraine and its allies must navigate the dual challenges of the conventional military threat and the looming danger of a nuclear fallout (Ahn, 2023). By keeping the threat of a nuclear incident in the global consciousness, Russia effectively leverages the complexities and fears associated with nuclear technology to achieve strategic objectives. The uncertainty surrounding the conditions of the power plant

amplify the perception of danger beyond the physical threat which basically makes Zaporizhzhia a tool in Russia's hybrid warfare efforts.

# 6. Different Countries, Different Challenges

While non-state actors may also leverage hybrid CBRN threats, this paper does not directly focus on them. Following the investigation into the CBRN environment and examples of hybrid threats within it, this paper shifts its focus to specific countries. Specifically, it examines the capabilities of four state actors that enable them to use hybrid CBRN threats: the Russian Federation (Russia), the People's Republic of China (China), the Islamic Republic of Iran (Iran), and the Democratic People's Republic of Korea (North Korea). Due to the lack of transparency, as none of these countries openly share their capabilities, the discussions are fragmentary. It examines the countries' hybrid and CBRN capabilities to illustrate the potential risk of these countries being able to use hybrid CBRN threats.

## 6.1. Russia

In a recent statement, NATO warns about Russia's intensifying hybrid activities on Allied territory (NATO/OTAN, 2024d). Russia argues the West was first to deploy hybrid threat activities, often quoting the colour revolutions and the Arab Spring as examples of Western hybrid aggression (Crowther, 2021). For the West, in the early 2010s, the *Gerasimov doctrine* became central to the understanding of (Russian) hybrid warfare (Galeotti, 2014). However, the author, whose article coined the term, later urged Western understanding not to be built on this doctrine, as e.g., it was not even Gerasimov's interpretations, but ideas by Russian officers Chekhov and Bogdanov that were discussed (Fridman, 2019). Hybrid threats do not necessarily aim to achieve a specific outcome but simply division, destabilisation, and intimidation within the target. Russia's activities aim to erode trust in organisations, squander resources of the West and impede decision-making.

In contemporary times, Russia has successfully used hybrid threats to influence and weaken its adversaries. Examples can be found everywhere, e.g., Russia's "borderization" policy in Georgia (Seskuria, 2021), or Russia's disinformation campaigns that target the minority populations in Transnistria or the Gagauzians in Moldova (Kubica, 2024). Other examples are the countless interferences in Western elections (most infamously the 2016 U.S. elections (Office of the Director of National Intelligence, 2017)) and perpetual cyber-attacks in the Baltic countries (Nilsson, Weissmann, Palmertz, Thunholm, & Häggström, 2021). According to Hicks et al., apart from information and cyber operations, Russia's hybrid threats focus on political coercion and space operations, jamming NATO's GPS signals or lasering sensors from a Japanese satellite (Hicks, et al., 2019, p. 9). Recently, Russia is jamming more and more GPS signals which leads to many commercial flights being interrupted, like the two Finnair planes from Helsinki to Tartu, Estonia (Milne, 2024). Prior to the invasion of Ukraine, Russia enjoyed demonstrating its military capabilities through annual military exercises held in various military districts, namely Kavkaz, Zapad, Vostok, and Tsentr (Johnson, 2018). These exercises are still ongoing, and there is a renewed focus on who participates alongside Russia in them to signal alliance against the West. These demonstrations of power are critical activities for shaping the narrative, particularly against the narrative of Russia being isolated on the international stage.

Influencing happens on many levels and often through disinformation and fear. Notably, the use of deceptive measures was already part of the Soviet Cold War tool kit (Lasconjarias & Larsen, 2015). As the paper focuses on hybrid CBRN threats, using disinformation on CBRN topics was already utilised by the Soviet Union. One infamous example is Operation Infektion/Denver, the attempt of the KGB and the East German security services to spread the narrative that HIV and AIDS are biological weapons created by the U.S. (U.S. Department of State, 2023). Building on the fears related to CBRN is something that Russia's hybrid techniques use to their advantage. Disinformation about CBRN by the

Kremlin is extensive, ranging from the U.S. and Ukraine training bats to carry biological weapons to Russia to human experiments having turned Ukrainian soldiers into monsters (U.S. Department of State, 2023). Lastly, there is the example previously discussed about the U.S.-funded biological laboratories. The disinformation and utilisation of fear around CBRN can also be seen relating to nuclear capabilities. As the successor of the Soviet Union, Russia still has a vast nuclear repertoire. According to Reuters, Russia possesses the most nuclear warheads in the world, around 5580 (Faulconbridge, 2024). Since the full-scale invasion of Ukraine in the beginning of 2022, the Kremlin, Putin, and others have often used nuclear threats as means to discourage Western support to Ukraine (Pifer, 2023). Russia has been using its own nuclear arsenal in a hybrid manner to create fear and impair decision-making in the West threatening with the use of nuclear weapons or using the fear around the Zaporizhzhia power plant to their advantage. Furthermore, there have been reports of the Russian military using CS gas to support their attacks on Ukraine, thus, intentionally breaking the rules outlined in the CWC (Badshah, 2024). Moreover, Russia refers to Ukraine as a "special military operation." The extent to which the case can be justified based on the law enforcement aspect, which states that riot control agents are legal in law enforcement actions, is showing how Russia uses rhetoric and language to circumvent international rules. It emphasises Russia's use of international regimes and law to its advantage, presenting it's narratives as alternative interpretations and for legitimising their actions. The use of CS gas has mainly a psychological effect on the soldiers and the public as it is not as lethal as other chemical agents, but coupled with Russia's use of lethal chemicals, like the Skripal Novichok example, demonstrate its lowered threshold to use such materials, while still causing fear and reducing combat effectiveness and demonstrating power.

**As it can be seen, Russia has advanced capabilities in both conventional and unconventional warfare, including cyber warfare, disinformation campaigns, and the use CBRN agents. It employs a hybrid warfare approach to achieve its strategic objectives. Its motivations for engaging in hybrid CBRN threats include undermining Western democracies, challenging NATO's cohesion and credibility, and asserting its influence in regional and global affairs.**

## 6.2. China

Contrary to the Western binary perspective of war and peace, the Chinese strategy embraces a dialectic approach, often grounded in stratagems (Giannopoulos, Smith, & Theocharidou, 2021, p. 21). This perspective does not draw a distinct line between war and peace; instead, it views them as interconnected. What the West calls hybrid warfare, China refers to as *unrestricted warfare* (Jash, 2019, p. 101). Jash argues that China's goals is to shift from conventional warfare to the political domain, employing societal forces such as public opinion, legal systems, and leadership of adversaries (Jash, 2019, p. 103). Additionally, in the Chinese view, predominantly state actors engage in these activities, with non-state actors acting merely as puppets of state entities (Saalman, 2021, p. 102). Compared to Russia, China has a larger military budget, facilitating modernisation, and a more extensive technology and STEM-based industry, which boosts its military capabilities (Cordesman & Hwang, 2020, p. 4). Central to the development of these capabilities is the concept of military-civil fusion aiming to transform the scientific defence industry (U.S. Department of Defense, 2023, p. IV).

The modernisation has also shifted a large focus on cyber capabilities which are used in the hybrid warfare approach. The "Digital Silk Road" allowed China to have access to vast amounts of data through the installed fibre optics, which enables the acquirement of intellectual property and conduct of industrial espionage (Hicks, et al., 2019, p. 8). One example of alleged Chinese cyber activities is the U.S. Office of Personal Management (OPM) data breach discovered in 2015. Hackers linked to the Chinese government infiltrated the American OPM, gathering personal information of millions of federal employees (Fortra, 2015). Another incident occurred in 2016, when the U.S. accused the *Chinese General Nuclear Power Group* of having stolen nuclear secrets (Cordesman & Hwang, 2020, p. 23). The incident highlights Chinese state-sponsored cyber espionage efforts as part of its hybrid strategy, even regarding the CBRN environment. Additionally, there are aggressive military demonstrations in the South China Sea and the creation of artificial islands with the goal of increasing influence and projecting power (Jash, 2019, pp. 98, 100).

The ongoing modernisation of the Chinese military highlights the potential for hybrid CBRN threats. Currently the Chinese nuclear arsenal comprises around 500 operational nuclear warheads, with plans

to double the number by 2027 (U.S. Department of Defense, 2023, p. VIII). According to the *U.S. Department of Defense*, information dominance is a crucial preliminary step in Chinese military strategy, with increasing integration of AI and advanced technology to develop *intelligent warfare* (U.S. Department of Defense, 2023, p. VII). Additionally, China's growing CBRN capabilities, coupled with its use of disinformation to influence public opinion, present future risks. For instance, China used disinformation during the COVID-19 pandemic to obscure discussion about the virus's origins (Cordesman & Hwang, 2020, p. 13). Dual use equipment is pivotal in the modernisation, aiming to enhance defence capabilities against conventional, nuclear and biochemical attacks (Saalman, 2021, p. 100). This has raised concerns about the development of biological and chemical weapons under the guise of research, and the weaponisation of existing research. Research on dual-use potent toxins and pharmaceutical-based agents raises questions about compliance with the BWC and CWC (U.S. Department of Defense, 2023, p. IX). Notably, recent research into marine-based neurotoxins has sparked worries about their potential use as biological weapons (Fitzgerald, 2024). Whether this research is intended to prevent poisoning from seafood or to develop new weapons remains a question, highlighting the dual-use dilemma. Still, all these developments underscore the complex and evolving nature of the threats posed by China's military modernisation that could also include hybrid CBRN threats in the future.

**China's focus on modernising its military and expanding its capabilities in areas such as biotechnology, cyber warfare, and conventional military power, indicates a cohesive approach that can also consider the possibility of hybrid CBRN threats, as in both areas capabilities are strengthened. China's motivations for engaging in hybrid threats include asserting territorial claims, countering perceived threats to its sovereignty through power projection, and attaining regional hegemony in the Indo-Pacific region by fostering economic dependencies and economic espionage.**

## 6.3. Iran

Iran's development of hybrid defensive and offensive capabilities is largely shaped by its historical experiences. The lessons drawn from the Iran-Iraq war (1980-1988) and the 2003 U.S. invasion of Iraq have significantly influenced Iran's contemporary force structure. The Iran-Iraq war exposed the weaknesses of Iran's conventional forces, leading to a strategic shift towards enhancing deterrence and defence capabilities. This shift involved strengthening relations with allies and proxies, building a guerrilla-like infrastructure, and advancing non-conventional methods such as drones, cyber warfare, and covert operations (Parsi, 2021, p. 234). Since 2016, Iran's offensive strategy has been emphasised, as reiterated by Supreme Leader Khamenei in a February 2022 speech, stating that offensive measures must be the response to Western hybrid warfare (Carl, 2023, p. 8). It is noticeable that Iran attempts to modernise their conventional weapon systems but is always restraint by budgetary boundaries (DNI, 2024, p. 19). Thus, it is their asymmetric capabilities, like their nuclear build-up, missile arsenal, and proxies that they rely on (Wasser & Matuschak, 2022). These developments underscore Iran's commitment to evolving its military tactics to address both current and future threats but also to use them in an offensive manner.

Iran projects much of its power through proxies and the so-called *Axis of Resistance*. Their support is extensive including supplying missiles and rockets to their proxies and members of the *Axis of Resistance* to destabilise the region (NTI, 2024). The Houthis are one of the groups that have used these missiles and UAVs for attacks on ships, ports and energy infrastructure (DIA, 2024, p. 3). Some of the drones are also provided to Russia and are used to terrorise the Ukrainian population and damage infrastructure (Mason & Holland, 2023). In Iraq, Iran has swayed governmental decision-making by supporting the Badr Brigades, asserting influence in Shi'a neighbourhoods, and adding pressure on adversaries using Improvised Explosive Devices (IED) and flying IEDs (Gardner, 2015). Actions through proxies like the Islamic Revolutionary Guard Corps (IRGC), Hezbollah or Houthis aim to shift the balance of power in the Middle East in Iran's favour while maintaining plausible deniability (Hicks, et al., 2019, pp. 2, 10).

In the cyberspace, Iran has engaged in significant cyber operation, including data deletions in Saudi Arabia in 2016 and 2017 and regular jamming of *Voice of America* and *BBC* (Hicks, et al., 2019, p. 11). Iran has also conducted cyber-attacks on other countries like Israel and attempted to influence the 2020

U.S. election through cyber- and disinformation operations (DNI, 2024, p. 20). After the Stuxnet incident, Iran recognised the importance of cyber capabilities and has since developed advanced skills, as demonstrated by the infrastructure attacks in Bahrain in July 2019 (Carl, 2023, p. 20). Iran often maintains plausible deniability by using hacker groups like the Black Swans, likely linked to the IRGC (Carl, 2023, p. 21). These actions illustrate Iran's capability and willingness to conduct cyber-attacks as part of its hybrid strategy, targeting critical infrastructure to retaliate against adversaries and advance its geopolitical interests.

The National Passive Defence Organization (NPDO), established in 2003 to strengthen Iran's resilience and infrastructure, has recently become a pivotal element of Iran's hybrid campaign, addressing cyber, biological, radiological, chemical, and economic threats (Nadimi, 2018). Notably, CBRN threats are managed through the same channel as hybrid and cyber threats. Iran has long aspired to develop its nuclear programme, which has caused international concern. As mentioned above, the Stuxnet malware deliberately delayed their programme. In regard to assessing Iran's access to biological and chemical weapons, it is more challenging than evaluating its nuclear capabilities. Although Iran is a signatory to the Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) and claims not to possess chemical weapons due to its experiences in the Iran-Iraq war, suspicions remain (NTI, 2024). The U.S. Office of the Director of National Intelligence stated that "Iranian military scientists have researched chemicals, toxins, and bioregulators, all of which have a wide range of sedation, dissociation, and amnestic incapacitating effects" (DNI, 2024, p. 19). While open-source information makes it difficult to fully assess Iran's CBRN capabilities, it does not imply that these capabilities are undeveloped.

**Iran has ameliorated their hybrid and nuclear capabilities to enhance its position in the Middle East and affect its opponents, relying on unconventional methods to due to the budgetary constraints. Iran possesses capabilities in asymmetric warfare, including support for proxy groups, cyber attacks, and potential access to chemical and biological weapons. Iran's motivations for engaging in hybrid CBRN threats include regional power projection, countering perceived threats to its regime stability, and challenging Western influence in the Middle East.**

## 6.4. North Korea

The last country to be discussed is North Korea. Its hybrid threat activities evolve around cyber operations and provocations to show the strength of the state and the ruling Kim family. Overall, North Korea is very isolated in the international realm and the regime aims to keep internal stability despite food insecurities and the absence of consumer goods (Bennett, et al., 2022, pp. 3-4). Reasons for isolation are the North Korean ideals of *Juche* (self-reliance) and *Songun* (military first) that have been guiding North Korea since its foundation in 1948, but also the vast list of UN sanctions that have been imposed on the country since they withdrew from the Non-proliferation Treaty in 2003 and started testing nuclear weapons in 2006 (CFR.org Editors, 2022). These sanctions have contributed to the economic difficulties that North Korea is facing. The country is trying to circumvent them by illicit activities, particularly in the cyberspace.

The North Korean cyber operations' main goal is to get access to funds and money. The money is needed to support the regime's ambitious WMD programme (DNI, 2024, p. 21). Already Kim Jong-un's father Kim Jong-Il saw WMD as means to preserve peace (Bennett, et al., 2022, p. 6). Most recently the attacks have been focusing on crypto-currency companies and allegedly made around $3.2 billion (Lee, White, & Jones, 2023). Other attacks have been aimed against critical infrastructure, military, governmental and private networks, as well as financial institutions (CFR.org Editors, 2022). The Lazarus Group is an infamous hacker group that is allegedly connected to the North Korean military intelligence and is possibly behind the 2014 Sony Picture Entertainment hack, the 2018 Cosmos Cooperative bank heist, and the WannaCry cyber attack (Lee, White, & Jones, 2023). The 2017 WannaCry Ransomware attack infected hundreds of thousands of computers worldwide, encrypting data and demanding ransom payments in Bitcoin (BBC, 2017). The incident underscored North Korea's willingness to use cyber-attacks as part of its hybrid strategy to fund its illicit activities, evade international sanctions, and exert pressure on its adversaries.

North Korea's capabilities in space-based systems jamming are notably advanced with South Korea being the most frequent target. According to Kicks et al., North Korea is “the most prolific space-based systems jammer in the world” (Hicks, et al., 2019, p. 12). These actions indicate a certain level of competence. However, assessing North Korea’s full capabilities is challenging due to its isolation. North Korea leverages this uncertainty to magnify the impact of its provocations and strategically manipulate perceptions by displays of power through nuclear weapon testing. The nation remains de facto non-transparent with military assets hidden in underground facilities to avoid satellite detection (Bennett, et al., 2022, p. 19). This strategic opacity complicates efforts to accurately evaluate the extent of North Korea's military capabilities and intentions.

North Korea’s provocative actions are primarily driven by its nuclear programme, which garners significant media attention and raises concerns about regional security on the Korean Peninsula. In the eyes of the Kim dictatorship, it is an important guarantor and object of national pride (DNI, 2024, p. 21). As mentioned above, nuclear testing started in 2006, and estimations predicted that North Korea had around 100 nuclear weapons in 2022 (CFR.org Editors, 2022). What was noted in the most recent Annual Assessment from the U.S. Office of the Director of National Intelligence is that North Korea is in an increasingly closer working relationship with Russia and China, visible through state visits and the import of dual-use goods which are violating UN sanctions (DNI, 2024, pp. 21-22). The regime's use of VX nerve agent in the assassination of Kim Jong-Nam in Malaysia in 2017 exemplifies its capability to deploy chemical weapons for strategic impact. The older brother of Kim Jong Un was killed with VX in Malaysia in 2017 by two women who smeared different chemicals on his face which interacted together (Ellis-Petersen, Lumpur, & Haas, 2019). Most estimations claim that North Korea’s chemical arsenal comprehends around 2500 to 5000 tonnes of chemical weapons, mostly sarin, yet some argue it is already more than 5000 tonnes (Bennett, et al., 2022, pp. 11-12). While North Korea's biological weapons stockpiling remains unverified, South Korean and U.S. defence assessments suggest they have production capabilities, including potential agents like anthrax and Korean haemorrhagic fever (Bennett, et al., 2022, p. 29). These biological weapons may be concealed within dual-use production facilities like historical practices observed in the Soviet Union and Iraq, where anthrax production masqueraded as bacillus thuringiensis biopesticide manufacture (Bennett, et al., 2022, p. 30). These hybrid and CBRN capabilities underscore the complex threat landscape posed by North Korea, necessitating vigilant monitoring and international cooperation to mitigate risks and ensure regional stability.

**North Korea has developed nuclear weapons and ballistic missile capabilities, and has a history of provocative behaviour, including cyber-attacks and use of chemical weapons. Its motivations for engaging in hybrid CBRN threats include regime survival, financial support, deterring perceived threats from regional adversaries and the United States, and extracting economic and political concessions from the international community.**

# 7. NATO’s CBRN Strategic Enablers in the Light of Hybrid Threat Activities

The second part of the paper focuses on the implications of hybrid threats for CBRN defence. The 2022 NATO CBRN Defence Policy mentions six strategic enablers that aid deterrence and defence against CBRN threats. Within the framework of these strategic enablers, the following part underlines important parts integral for countering hybrid CBRN threats in the present and future. By doing so, the paper supports the position of these enablers within CBRN defence, admittedly, as political tools, yet, also as signposts for crucial aspects of future defence considerations. Furthermore, by addressing the topic of hybrid CBRN threats structured through these enablers, the author wants to show how hybrid threats and CBRN threats are not separate but intertwined and consequently, how addressing them needs to be done in a comprehensive manner which reflects the state of the global threat environment. This part

identifies some gaps in current preparedness as well as necessities for sustainable resilience. Most of the information included in this part of the paper is collected from discussions and interviews with experts from the JCBRN Defence Centre of Excellence and academia. The notes and transcripts of the conversations can be found in the annex of the paper to get some more insights; however, they were made anonymous.

## 7.1. Shared Understanding

The first strategic enabler is called “shared understanding”. In the context of NATO which consists of 32 member states, shared understanding is essential for not only rapid decision-making but also vital for achieving NATO’s defence and deterrence goals. Shared understanding is also important, as hybrid and CBRN threats can both have cross-border effects. With CBRN threats, the historic case of the Chernobyl power plant has demonstrated that accidents involving such infrastructure can lead to radiation spreading across borders and even the Iron Curtain. More recently, the globalised world witnessed the COVID-19 pandemic, which, in the timeframe of a few months, affected every state regardless of its governmental structure, strategic alliances or economic might. Coupled with hybrid threats, the overall situation becomes very complex. This difficulty is further aggravated by the cyber domain. The cyber domain and the virtual realm do not adhere to borders and the way they affect people is not straightforward. Disinformation campaigns conducted through the cyber space affect populations not visibly, but indirectly through the online content they consume, which influences their opinions and convictions. It needs to be highlighted again that countering hybrid CBRN threats remains mainly a national responsibility; however, the gravity of the problem demands a supportive element in the form of cooperation and exchange between countries in order to find over-arching solutions. Here, shared understanding clears the path to enhance this cooperation.

The CBRN environment is often undervalued in defence. Some say attention is often only paid to CBRN risks and threats when accidents or challenges occur, such as the reactor failure in Fukushima, terrorist groups like ISIS gaining access to mustard gas and chemical weapons or endemic outbreaks like Ebola and Zika.[4] Thus, generally ameliorating threat awareness is important. Many different aspects play into shared understanding, all with the aim of enhancing threat awareness. Two mechanisms are central to achieving this within the context of hybrid threats in the CBRN environment: information sharing and intelligence sharing.

Information sharing is important, as hybrid threats often target the public. Thus, building and raising their awareness of the threat must be promoted and sustained. Hybrid threats have destabilising effects on society and preventing these effects has a lot to do with uncovering seemingly hidden narratives or polarising misinformation. With the changing information environment, information sharing becomes useful for surpassing the disinformation.[5] Disinformation often starts on a small scale, e.g. in local media or unimportant information sources and spreads from there.[6] Thus, fact-checking and educating the public is crucial. Inspiration can be drawn from initiatives like *EUversusDISINFO* or countries like Finland, which has made it part of its curriculum to foster critical understanding and critical consumption of information.[7] Also, like in the case of the Skripal poisoning, open-source investigative groups such as *Bellingcat* have proved valuable. A second important reason for ameliorating information sharing is that nowadays people are surrounded by vast amount of information that influences their perspective of reality. There is an information overflow and things like photographs, that used to be considered as a proof of or against a situation can no longer reliably serve this purpose.[8] How can it be determined if someone is only bluffing or if the threat is real? One example highlighting the issue in the paper are Russia’s nuclear threats in the current war.

The other mechanism for enhancing threat awareness and establishing shared understanding among allies or within NATO is intelligence sharing. NATO defines intelligence as “the product resulting from the directed collection and processing of information regarding the environment and capabilities and

[4] Interview 4
[5] Ibid.
[6] Interview 8
[7] Interview 7, Interview 8
[8] Interview 1

intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers" (NATO Standardization Office, 2022). Intelligence is a national asset of any government. For shared awareness, the most important aspect of intelligence is intelligence-sharing. Regarding hybrid threats it is recommended to cooperatively identify these threats and respond to them effectively. Intelligence sharing helps with informing the decision-makers and governments as well as supporting the military with situational awareness. According to the official NATO Terminology database, situational awareness is "the knowledge of the elements in the battlespace necessary to make well-informed decisions" (NATO Standardization Office, 2012). In the hybrid environment, the lines between war and peace are blurred and the conditions of the battlespace are altered, deliberately misleading and confusing. In this case the understanding of battlespace might need to be thought of in the bigger picture of the general security environment.

The intelligence enterprise, represented beside others also by NATO Intelligence Fusion Centre (NIFC), the Joint Intelligence and Security Division (JISD), and SHAPE J2, form the core of the enterprise and a hub for intelligence production and sharing in NATO.[9] Intel FS (functional services) is a platform for collection, dissemination and the use of intelligence among NATO nations. One of the tools is the IRM&CM Tool where stakeholders can submit RFIs (requests for information) for filling intelligence gaps.[10]

Nevertheless, intelligence sharing is not as straightforward as it might appear for a multitude of reasons which affect current effectiveness of intelligence sharing. The primary obstacle to effective intelligence-sharing is trust, as states are often hesitant to share what are ultimately sensitive national assets.[11] Also, as Janine McGruddy phrased it: "intelligence suffers from a paradox – it is only valuable when shared with those who need it, but the more it is shared the more it risks being compromised" (McGruddy, Fall 2013, p. 215). Other constraints with multilateral intelligence sharing are over-classification, disclosure, and oversight (Gorden, 2017, p. 19). Whereas overclassification is self-explanatory, disclosure refers to disclosing sources or collection methods. Oversight refers to the fact that these aspects need to be overseen to maintain standards balancing the risks of sharing, minimizing the use of illegitimate collection methods and ensuring the prevention of sharing with third parties. But when it comes to hybrid CBRN threats, intelligence is crucial to get ahead of disinformation campaigns or reveal other hybrid activities and attribute them to their source. CBRN, however, is a highly specialised field and often lacks the requisite number of technical specialists and intelligence experts.[12] Potentially, in the future, AI can support intelligence collection and fill the gaps of missing personnel, but as of now, it remains a future development.[13] Concerning CBRN intelligence, there is also one specific problem that was mentioned. CBRN-related intelligence is often not properly labelled in intelligence sharing platforms and consequently not drawn to be seen by the right people.[14]

To sum up, shared understanding is fundamental for any attempt at preventing or countering hybrid CBRN threats. To reach shared understanding, information and intelligence sharing are fundamental. Sharing information to a greater extent has become necessary due to the changing information environment with the bigger volume of information online. It is important to provide trusted sources to share information to limit the influence of disinformation. Intelligence sharing is another aspect that guarantees staying ahead through exchanging important information and analysis on the perception and level of threats. Great significance lies in having a shared perception of the threat, situational awareness, and operational picture as it guides coordination efforts, and the consensus strengthens the partnership between allies.

***Recommendation 1: Enhance information sharing and public threat awareness on hybrid CBRN threats in and among member states and partners to curtail the spread of polarising adversarial disinformation.***

[9] Interview 6
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Ibid.

***Recommendation 2: Improve media literacy through different initiatives to promote and protect fundamental values like freedom, democracy and the rule of law and preventatively decrease the effectiveness of disinformation.***

***Recommendation 3: Strengthen the CBRN intelligence community and boost (CBRN) intelligence sharing on the NATO level through addressing issues such as limited capacities and inadequate tagging.***

## 7.2. Capacity-building for Military and Civilian Personnel

Capacity-building is based on the assessment of the viability of perceived threats. This enabler is therefore connected to threat awareness and the previously mentioned strategic enabler – Shared Understanding. There is a need for interdisciplinary approaches and flexible capabilities in hybrid CBRN defence that can be adapted to counter evolving threats. All these aspects raise the significance of resilience in the current security environment against the multitudes of threats.

Training and education are the backbone of capacity-building. Integrating hybrid threats into CBRN training is important as they alter the conditions of the battlespace. The tools used to disrupt and undermine are constantly diversifying, offering novel and increasingly damaging opportunities for militarily inferior actors (Bilal, 2024). Regarding the education aspect, there needs to be a focus on strategic risk and crisis communication, to be able to counter disinformation early on. This will be explained in more detail in chapter 7.4.

For countering hybrid CBRN threats, high priority needs to be placed on interoperability and civil-military cooperation, which is defined as "the co-ordination and co-operation between the military and civil actors, including national population and local authorities, as well as international, national and non-governmental organizations and agencies" (NATO Standardization Office, 2022, pp. 6-1). In CBRN incidents, a general rule is that approximately 80% of the responders will be civilian and 20% military.[15] This degree of civil-military interoperability must be established and rehearsed prior to the outbreak of a CBRN crisis. Central to this are joint exercises, enabling participants to plan, train and learn countering novel challenges together. According to an expert in strategic communication, consequence management actions will always first reflect the nation's own capabilities during crisis scenarios. Only after national capabilities are assessed, nations will consider bilateral agreements to draw upon external support, or to receive support from international organizations, e.g. the Euro-Atlantic Disaster Response Coordination Centre (EADRCC).[16] In case of training CBRN defence, there are national and multinational exercises that can be used as a platform to train one's capabilities, whereas on NATO-level exercises, there must be more attention paid to CBRN defence during major exercises, as it is determined in SHAPE directives for CT&E (Collective Training & Exercises).[17] On an operational and strategic level in NATO exercises, cyber domain and influence operations are very popular for training as they are easily scripted. Examples of such exercises include STEADFAST DETERRENCE, STEADFAST DUEL, AND STEADFAST DAGGER.[18] However, hybrid threats scenarios during these exercises usually focus on cyber threats and are not necessarily related to CBRN. Some exceptions are scenarios in which cyber is used as a trigger for CBRN incidents or in which disinformation is surrounding a CBRN incident.[19] CBRN threats remain mainly a national responsibility, however, it would be advantageous to include more CBRN elements, ideally coupled with hybrid threats, in NATO major exercises.

A reoccurring problem with capacity-building is the topic of funding. This is not a CBRN specific issue, considering that for many years defence budgets have been an often-disputed topic among member countries. Since Russia's annexation of Crimea and particularly following Russia's full-scale invasion of Ukraine, defence budgets have increased in NATO countries and this year 23 out of the 32 NATO

[15] Interview 5
[16] Ibid.
[17] Interview 3
[18] Interview 5
[19] Ibid.

countries will spend the 2014-agreed 2% of their respective Gross Domestic Product (GDP) on defence (Landay, Psaledakis, & Hunnicutt, 2024). In many discussions for this paper, investments for CBRN defence were often compared to insurance policies, as the usefulness of investments is questioned until the event of a crisis occurs.[20] Any investment is contemplated and weighed up against other options. But this can lead to gaps in preparedness such as stockpiles, as the necessary funds for them is not provided. It was highlighted that having adequate stockpiles available with individual protective equipment such as protective garment and respirators for everyone would be ideal but given the budgets it may be unlikely.[21] Hybrid threats exploit vulnerabilities across multiple domains, including political, economic, and technological. Thus capacity-building is important for developing preparedness and building resilience against hybrid tactics through comprehensive training and exercises that simulate integrated responses to complex scenarios involving CBRN incidents alongside other forms of hybrid aggression for which sufficient funding is crucial to be adequately prepared.

***Recommendation 4: Increase CBRN elements in NATO strategic exercises and couple them with hybrid threats to ameliorate preparedness for hybrid CBRN threats. This should strengthen NATOs cross-disciplinary efforts and capabilities, as the organisation needs to develop the ability to quicker adapt to novel challenges and respond to emerging threats.***

***Recommendation 5: Enhance civil-military cooperation in CBRN defence and security to counter hybrid CBRN threats as this liaison is critical during an incident and must be reinforced on a regular basis to maintain an adequate level of preparedness.***

***Recommendation 6: With renewed threat awareness, allocate a larger portion of the NATO military and national budgets to CBRN defence.***

## 7.3. Partnerships and Outreach

In the previous section, the significance of engaging civil and military actors in defence and deterrence processes was already highlighted. Hybrid threats require a whole-of-society response, involving cooperation with a wide range of stakeholders beyond traditional defence and security actors. In relation to NATO, there are many bilateral partnerships or agreements with international organisations like the United Nations and the European Union to coordinate CBRN-related civil preparedness and crisis management activities or the implementation of UN Security Council Resolution 1540 (2004) on the prevention of the proliferation of CBRN weapons (United Nations Office for Disarmament Affairs, 2024).

There are cooperations through EU organisations like the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO) for training and protection mechanisms. Having investigated EU-NATO cooperation regarding hybrid threats, Filipec found out that “cooperation is vital for connecting the civilian background of the EU with the military perspectives of NATO”, but the extent to which these opportunities are used depends on the nation states as it is up to them to decide how to optimise their capacities (Filipec, 2023, p. 46). The countries themselves and various organisations are also constantly involved in partnership and outreach efforts.

In the case of the JCBRN Defence CoE, it engages with different actors in many ways, e.g. during their annual conference or through their courses.[22] This year, for instance, the COE offered a course for Ukrainian first responders and further contributes by delivering a consequence management course in the MENA countries.[23] Often, NATO facilitates funding and course requests for these initiatives, like in the case of the course for Ukrainian first responders which was requested by Supreme Headquarter Allied Powers Europe (SHAPE).[24] Another example for partnership and outreach within NATO is the Science for Peace and Security Programme which “offers funding, expert advice and support to tailor-made, civil security-relevant activities that respond to NATO’s strategic objectives” (NATO/OTAN,

[20] Interview 1
[21] Interview 1, 3, 4
[22] Interview 5
[23] Ibid.
[24] Interview 5

2024c). The renewed priorities include CBRN management and defence against hybrid threats. (NATO/OTAN, 2024b)

Going into more detail for partnerships and outreach is not necessary for this paper. The concept is self-explanatory, and it is practised. In the context of partnership and outreach, it is important to engage civil society, the private sector, academia, and international organisations to counter hybrid tactics, including disinformation campaigns aimed at undermining public trust and exacerbating CBRN threats. Therefore, civil-military cooperation plays an important role. It was mentioned before, but one last important aspect of the civil-military cooperation are multinational exercises. These exercises, like Steadfast Defender, strengthen collective defence and enhance the resilience of allied and partner nations against CBRN threats, including those with cyber components, fostering a more secure and interconnected security environment.

***Recommendation 7: Boost preparedness for hybrid CBRN threats by engaging with different stakeholders.***

***Recommendation 8: Continue to enhance partnership and outreach efforts.***

## 7.4. Strategic Communication and Public Diplomacy

Hybrid threats often seek to exploit divisions within societies and weaken public confidence in democratic institutions, thus, putting renewed priority on open and clear communication. Because of that, transparent and coherent messaging to counter disinformation and build public resilience against hybrid tactics is crucial. Strategic communication further helps with raising awareness about hybrid threats, including the potential intersection with CBRN incidents, and promoting civil resilience and preparedness.

New communication technologies, particularly regarding the internet, have changed the information landscape forever. They have also changed communication. It was highlighted in one of the interviews that communication goes beyond the framework of a simple sender-receiver relationship and nowadays has rather dynamic and "participatory" characteristics.[25] These developments have complicated communication, as the truth seems to be increasingly out of reach and constantly contested. That's why it is important to know how to get ahead of false narratives nowadays to remain effective in debunking them. Therefore, it is important that communication remains clear and unambiguous as it can otherwise easily lead to confusion. An example given was the confusion surrounding mask wearing during the COVID-19 pandemic.[26] In the beginning of the COVID-19 pandemic, it was not encouraged to buy masks, since the available resources were mainly needed by the medical personnel, and it was important to avoid hoarding of masks by the public. The situation changed when masks became more widely available, and it was openly communicated to wear masks as protection mechanisms, but people were hesitant and confused partially due to the initial nature of the communication. As mentioned in a previous section, people have constant access to information. That's why in crisis situations, clear communication is crucial, as the alternative would be people finding the alternative answers (and be receptive to dis- and misinformation) or creating their own narratives, especially in situations when hybrid threats are connected with CBRN threats, aiming to confuse public on purpose.

There are many different aspects to strategic communication. To some extent, deterrence can be regarded as a tool of strategic communication.[27] It provides awareness and helps with trust and reassuring the public that recovery and defence are possible in case of emergencies. According to the NATO Strategic Communications Centre of Excellence, NATO strategic communications is "the coordinated and appropriate use of NATO communications activities and capabilities in support of Alliance policies, operations and activities, and in order to advance NATO's aims" (NATO Strategic Communications Centre of Excellence, 2020). It includes different activities, namely public diplomacy, public affairs, military public affairs, information operations, and psychological operations that are

[25] Interview 8
[26] Interview 5
[27] Interview 7

contributing to the successful implementation and coordination of NATO strategic communication in NATO operations. Public diplomacy is "NATO civilian communications and outreach efforts responsible for promoting awareness of and building understanding and support for NATO's policies, operations and activities, in complement to the national efforts of Allies" (NATO Strategic Communications Centre of Excellence, 2020).

Regarding CBRN risk communication, the three different phases of an incident are preparation, crisis, and recovery.[28] In the preparation phase, communication is flat, and the focus is stakeholder engagement and public engagement making sure that in the event of an incident communication lines are already established. In comparison to the preparation phase, for crisis communication it is not orientated on flat communication lines but on a top-down approach. A strategic communicator limits the time of crisis communication as much as possible, but to be able to do that, they need to be well-prepared in advance. After the crisis, communication should open up immediately. During a crisis event, messaging intends to persuade people and influence their behaviour. It is coordinated but not centralised and needs to follow the rule of "one message, many voices". It is said that first responders are the best communication channels in severe emergencies. Well-informed and well-trained first responders can be the key element to good risk and crisis communication, yet as of now, they often remain an unused capacity in this regard. From crisis to recovery, the communication lines flatten again. The focus is on supporting responders and the affected stakeholders in their recovery.

These aspects need to be reflected in training and education to allow for sufficient preparation. Communication aspects need to be included in every emergency exercise. It is also recommended to have exercises in which the ones involved need to explain their actions.[29] Also including other stakeholders, such as the local community or journalism educational institutions, in such exercises or training activities is advantageous to better account for the reality of such scenarios in the training.[30] At the CoE's consequence management course, a full day of the course is dedicated to strategic communication. The participants learn how communication breakdowns can occur and how to provide clear messaging in a time of crisis. The participants are filmed giving an incident briefing and then the video is evaluated.[31]

In one of the interviews, it was argued that a strong focus on public trust as an objective of communication is counterproductive.[32] Overemphasising public trust is problematic because it obstructs effective communication. If leaders obsess over their public image and aim to create and maintain public trust as an objective of their communication, they will be afraid to communicate gaps in knowledge and uncertainties and therefore, the resulting communication will often be too late. Therefore, public trust is not a good objective for strategic communication but merely a byproduct of good work.

To sum up, new communication technologies have transformed the information landscape into a complex, participatory space in which staying ahead of false narratives is crucial. Preparation focuses on stakeholder and public engagement, ensuring effective communication lines. In crises, messaging becomes top-down to persuade and influence behaviour, whereby well-trained first responders could play a key role. Recovery reverts to inclusive communication, supporting affected populations. Effective communication during emergencies, such as clear messaging and timely information sharing, is crucial for maintaining public trust and managing crises effectively which requires planning considerations.

***Recommendation 9: Maintain and establish effective lines of communication at all levels to ensure their availability in the event of an incident and to signal preparedness. It is critical to engage stakeholders and provide strategic communication training to first responders.***

***Recommendation 10: In the event of a crisis, communicating about uncertainties and gaps in knowledge is preferable to communicating insufficiently or too late, as it allows false narratives to emerge and spread.***

---

[28] Interview 8
[29] Ibid.
[30] Ibid.
[31] Interview 5
[32] Interview 8

## 7.5. Scientific and Technical Collaboration

Technical collaboration is an important aspect of partnership and outreach, discussed in one of the previous sections. On the NATO level, there is the NATO Science and Technology Organisation (STO) to enhance the collaboration. Hybrid threats may involve the use of advanced technologies, including cyber capabilities, UAVs, and biotechnologies, to amplify the effects of CBRN incidents. In the context of scientific and technical collaboration, the focus needs to be on leveraging innovation and research capabilities to develop countermeasures against emerging hybrid threats, including the development of advanced detection technologies and cybersecurity measures to protect critical infrastructure from hybrid attacks. Depending on the intent behind using the emerging and disruptive technologies (EDTs), they can have negative or positive implications for new defence technologies and countermeasures and come with a long list of challenges.

Firstly, the challenges will be covered. New technologies and innovations have evolved the CBRN threat and facilitated the production and proliferation of CBRN materials. The aspects of masses of information freely flowing and consequently disinformation spreading faster due to the internet has already been discussed, as well as the opportunities 3D printers offer in the production of weapon parts and CBRN dissemination devices. Additionally, autonomous systems and robotics alter the tangibility of an attack, as distance and exposure become less of an issue. Robotic equipment can be used to handle hazardous materials, e.g. to release them without risking human operatives. Furthermore, DNA is available for purchase online and can be used for the synthesis of pathogens. Moreover, the evolving nature of AI alters the realm of possibilities within the CBRN environment, as synthesisers paired with AI can design and synthesise many new agents without any person behind the process. Also, AI can overcome the constraints of conventional thinking. Specifically, AI could be tasked to generate new ways to conduct a successful terror attack including ways that we might not think about. AI could also be used to identify vulnerable populations or infrastructure for more precise or effective CBRN attack.[33]

As much as the challenges are daunting, new technologies also offer opportunities to boost defence capabilities. Novel capabilities in detection, decontamination, forensics, individual and collective protection, knowledge management, medical countermeasures and more offer new avenues for countering CBRN threats. Technology advances in detection, stand-off detection and drone detectors for aerial surveillance offer possibilities for decision-making in a timelier manner.[34] It was mentioned that rather than waiting to identify gaps, forward-thinking problem-solving should be promoted to facilitate more efficient use of new technologies.[35] Creative solutions can be discovered by taking into account everything that is available and screening research publications for objects or mechanisms that can be modified for military use. Experts say that using AI in this process would be beneficial because it could scan thousands of research papers faster than humans.[36]

That last point already hints at one of the various challenges that accompany the new developments in science and technology. Analogous to the challenges mentioned in capacity-building, investments are limited in enhancing current capabilities due to lower casualty numbers related to CBRN incidents which compared to those caused by other threats lead to less focus on CBRN defence in the overall defence picture. NATO STO offers different programmes that aim to maintain NATO's military advantage. However, it was identified that in order to stay ahead of the game shift in cycle of industry-science-military must occur as well as a decrease in field bias. Current scientific and technical collaboration has a narrow focus on military-focused science and does not look outside of the inventions in the military field which can create a bubble.[37] It would be beneficial if researchers that could advance the military would approach them directly, but many scientists do not think about military application of their inventions. However, scientific findings from many different sectors like biotechnology, food, agriculture, or the car industry could hold a potential for the military. The war in Ukraine has proved that if the need

[33] Interview 3
[34] Interview 4
[35] Interview 3
[36] Interview 3, 4
[37] Interview 3

arises, any existing technology can be repurposed as a weapon.[38] The last challenge of scientific and technological collaboration concerns cooperation with the industry. On one hand, sharing of information, knowledge and intelligence is limited as highlighted earlier. On the other hand, overseeing dual-use technologies is a complex endeavour. To mention one example, the mechanisms in place for monitoring dual-use technologies are based on our understanding of what can be used for both purposes; however, other nations, such as China or India, may have different perspectives that may not considered.[39]

NATO must leverage the STO to enhance collaboration and address the complexities of hybrid threats, which involve advanced technologies like cyber capabilities, UAVs, and biotechnologies. These threats have the capability of amplifying CBRN incidents, necessitating innovative countermeasures, detection technologies, and cybersecurity for critical infrastructure. However, technological advances not only bring opportunities but also pose challenges, facilitating the proliferation of CBRN threats and enabling sophisticated, less detectable attacks using AI, robotics, and 3D printing. A proactive, interdisciplinary approach is essential, integrating civilian innovations and overcoming barriers in the industry-science-military cycle. Broader collaboration is crucial, as seen in the adaptive use of technologies in conflicts like the war in Ukraine.

***Recommendation 11: Advance the industry-science-military cycle to overcome field-bias, considering also scientific and technical findings in other sectors for military purposes.***

***Recommendation 12: Change the mindset from gap-orientated to forward thinking to improve the ability to think outside the box.***

## 7.6. Medical Support

Hybrid threats may involve the deliberate use of CBRN agents to cause mass casualties or disrupt healthcare systems. The 2022 NATO AJMedP-7 considers the effect of hybrid threats on the CBRN environment and consequently on medical support. It mentions hybrid as a possible operational environment (NATO Standardization Office, 2022, pp. 1-4) and considers the possibility that “an endemic disease or other type of environmental hazard may be exploited and used as a weapon but masked in a way to be mistaken as non-deliberate” (NATO Standardization Office, 2022, pp. 3-11). Other examples of hybrid threats affecting medical support can be attacks on first responders caused by population aggravated due to disinformation or casualty evacuation disrupted by drones (Granholm, Tin, & Ciottone, 2023, p. 244). Thus, there needs to be emphasis on the importance of preparedness and coordination among healthcare providers, emergency responders, and public health authorities to respond effectively to CBRN incidents perpetrated as part of hybrid tactics.

According to the AJMedP-7 “medical support is a function that encompasses the full range of medical planning and provision of medical and health services to maintain the force strength during the threat or occurrence or in the aftermath of a CBRN incident” (NATO Standardization Office, 2022, pp. 1-1). Granholm, Tin and Ciottone also argue that the example in Salisbury shows that the casualty number does not need to be high to strain response capacities (Granholm, Tin, & Ciottone, 2023, p. 243). They suggest using the counterterrorism medicine framework as a tool for hybrid, as it “can be used to analyse both hybrid warfare and terrorist events and … as a tool to mitigate, prepare, respond, and recover in hybrid situations” (Granholm, Tin, & Ciottone, 2023, p. 244). All these circumstances highlight the need for robust medical countermeasures, including vaccines, antidotes, and medical treatments, as well as training and simulation exercises to ensure readiness for hybrid CBRN threats. Concerning the exercises, the largest NATO exercise that focuses on interoperability between CBRN defence and medical forces in a CBRN environment is Exercise CleanCare. (NATO Standardization Office, 2022, pp. 7-3)

One significant part of medical support is the provision and development of medical countermeasures that can mitigate or reduce symptoms of CBRN events. Medical countermeasures can be vaccines, antidotes, potassium tablets or bronchodilators (ECHO, 2023). Their development can include the

[38] Interview 3
[39] Ibid.

creation of new drugs or the repurposing of existing ones. (Reddy, 2024, p. 261) The continuous development of medical countermeasures is important for effective preparedness. Continuous research is even more important against the backdrop of antibacterial resistance, a longstanding concern for public health. (Levy & Marshall, 2004) There are different endeavours into medical countermeasure research. One example is the U.S. organisation CEPI that is working on finding a way to generate a new vaccine for any 'Disease X' within 100 days (CEPI, 2024). They hope this milestone, paired with early warning, testing and limiting disease transmission, will make it possible to limit the impacts of a future pandemic with a faster roll-out of vaccines (Dr Hatchett, 2024). Considering previous discussion in this paper relating to the COVID-19 pandemic, vaccines became a target of disinformation. Thus, in the future, it is important to keep up public information and debunk mis- or disinformation to make sure that the existing medical countermeasures and medical support are not rejected on the basis of false information. Similarly, significance of stockpiles has been highlighted in an effort to ensure the availability of medical support in the case of an incident. On the NATO level, there are ambitions for enhancing the CBRN defence stockpiles, including medical countermeasures, pharmaceuticals, protective and medical equipment (NATO Standardization Office, 2022, pp. 3-10). The same aspirations are visible within the EU. Last year, the first rescEU CBRN strategic reserve was established (ECHO, 2023). The boosting of medical countermeasures and their provision is crucial for the response to accidental or deliberate CBRN incidents.

The last aspect that needs to be considered when it comes to the effects of hybrid threats on medical support is the vulnerability of healthcare systems. One recent example shows the vulnerability of medical infrastructure. In the beginning of June 2024, a malicious cyber operation affected many hospitals and GP services across London. The direct victim of the ransomware cyber-attack was Synnovis, a partner of many of the affected hospitals providing pathology services (BBC, 2024). The alleged group behind the attack is Quinlin, a Russian cyber gang that has operated for two years and attacked organisation before, such as courts in the Australian state of Victoria (Newton, 2024). The impact had consequences on the delivery of services like blood transfusions and led to medical procedures being cancelled (BBC, 2024). This shows that the disruptions caused can quickly escalate and affect many people. That's why it is important to have contingency plans and invest in software resilience in the contemporary world. The disruption of key services is one of the main characteristics of hybrid threats as it exploits vulnerabilities and has more far-reaching effects than the actual attack. But also, in the context of conflicts and war, health services are increasingly under attack. According to the Geneva Convention I and II, in war, certain civilian and military medical personnel are accorded special protection (Gillard, 2020). The protection of civilians, including of civilian medical staff, is a base of international humanitarian law. This rule seems to be less adhered to as for example the World Health Organization (WHO)) has recorded more than 1000 attacks on healthcare in Ukraine only within the first 15 months of the war (WHO, 2023). Hence, physical and cyber-attacks on health services and facilities are increasing, which has consequences for the provision of medical support and highlights the need for better defences.

***Recommendation 13: Boost research and stockpiling of medical countermeasures to be adequately prepared to respond to an incident, accidental or deliberate in nature.***

***Recommendation 14: Debunk disinformation regarding medical countermeasures and promote scientific exchange as a fundamental principle.***

***Recommendation 15: Strengthen the cyber capabilities of vulnerable critical infrastructure like hospitals or health services to protect them and maintain the provision of medical support.***

# 8. Overview of Recommendations

***Recommendation 1:*** *Enhance information sharing and public threat awareness on hybrid CBRN threats in and among member states and partners to curtail the spread of polarizing adversarial disinformation.*

***Recommendation 2:*** *Improve media literacy through different initiatives to promote and protect fundamental values like freedom, democracy and the rule of law and preventatively decrease the effectiveness of disinformation.*

***Recommendation 3:*** *Strengthen the (CBRN) intelligence community and boost CBRN intelligence sharing on the NATO level through addressing issues such as limited capacities and inadequate tagging.*

***Recommendation 4:*** *Increase CBRN elements in NATO strategic exercises and couple them with hybrid threats to ameliorate preparedness for hybrid CBRN threats. This should strengthen NATOs cross-disciplinary efforts and capabilities, as the organization needs to develop the ability to quicker adapt to novel challenges and respond to emerging threats.*

***Recommendation 5:*** *Enhance civil-military cooperation in CBRN defence and security to counter hybrid CBRN threats as this liaison is critical during an incident and must be reinforced on a regular basis to maintain an adequate level of preparedness.*

***Recommendation 6:*** *With renewed threat awareness, allocate a larger portion of the NATO military and national budgets to CBRN defence.*

***Recommendation 7:*** *Boost preparedness for hybrid-CBRN threats by engaging with different stakeholder.*

***Recommendation 8:*** *Continue to enhance partnership and outreach efforts.*

***Recommendation 9:*** *Maintain and establish effective lines of communication at all levels to ensure their availability in the event of an incident and to signal preparedness. It is critical to engage stakeholders and provide strategic communication training to first responders.*

***Recommendation 10:*** *In the event of a crisis, communicating about uncertainties and gaps in knowledge is preferable to communicating insufficiently or too late, as it allows false narratives to emerge and spread.*

***Recommendation 11:*** *Advance the industry-science-military cycle to overcome field-bias, considering also scientific and technical findings in other sectors for military purposes.*

***Recommendation 12:*** *Change the mindset from gap-orientated to forward thinking to improve the ability to think outside the box.*

***Recommendation 13:*** *Boost research and stockpiling of medical countermeasures to be adequately prepared to respond to an incident, accidental or intentional in nature.*

***Recommendation 14:*** *Debunk disinformation regarding medical countermeasures and promote scientific exchange as a fundamental principle.*

***Recommendation 15:*** *Strengthen the cyber capabilities of vulnerable critical infrastructure like hospitals or health services to protect them and maintain the provision of medical support.*

# 9. Conclusion

Threats in the CBRN environment have been, and will continue to be, combined in a hybrid manner. Chemical hybrid threats include new, difficult-to-detect chemicals that can be used maliciously, as in the Salisbury poisoning. Biological hybrid threats include impacts of the erosion of public trust in science and the health-care systems, as witnessed during the COVID-19 pandemic. Radiological hybrid threats could include cyber-attacks on critical infrastructure, which could be used to conceal the theft of radiological material suitable for a dirty bomb. Finally, nuclear hybrid threats include sabotage of nuclear facilities or exploiting public fear of nuclear incidents, such as in the case of the Zaporizhzhia power plant. State actors have increasingly expanded their CBRN capabilities and hybrid activities to strengthen their international influence and destabilise opponents.

The analysis of current preparedness revealed gaps and vulnerabilities in hybrid CBRN defence. It suggests enhancing information sharing and public awareness, improving media literacy to protect fundamental values, strengthening the intelligence community, increasing CBRN elements in NATO strategic or operational level exercises in combination with hybrid elements, enhancing civil-military cooperation, allocating a larger portion of budgets to CBRN defence, engaging with stakeholders, maintaining effective communication lines, and addressing uncertainties and gaps in knowledge in crisis communication. Furthermore, it also suggests fixing the industry-science-military cycle, switching to forward-thinking, boosting research, stockpiling of medical countermeasures, and promoting scientific exchange with non-military researchers. Lastly, cyber defence capabilities of vulnerable critical infrastructure like hospitals and health services should be strengthened to protect them and maintain medical support in case of a crisis.

CBRN threats and hybrid warfare are not novel challenges, and future initiatives must work to bridge the gap in their respective defence plans and capabilities. Resilience in the face of this combined challenge, ultimately, cannot be generated in an emergency, and it is only by leveraging multi-national cooperation across governments and, indeed, societies that NATO’s core tasks of deterrence and defence can be assured.

# Authors

## Author

**Paulina Frederike GOGACZ** completed her internship at the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence in 2024, following her earlier internship at the German Institute for Defence and Strategic Studies. She holds a Master's degree in Intelligence and International Security from King's College London. Currently, she works as a research consultant in the field of OSINT/SOCMINT for corporate security. She has a keen interest in civil-military cooperation and NATO, recognising that effective collaboration between military and civilian sectors is crucial for addressing complex security challenges and fostering resilience.

## Supervisor

**Linda VAŘEKOVÁ, MSc** is the Biological Defence Analyst at the Operation Support Department of the Joint Chemical, Biological, Radiological and Nuclear Centre of Excellence within the NATO CBRN Reachback. She is also a PhD student at the University of Defence where she works on her project focusing on analysis of epidemiological data from NATO missions. Her project aims to enhance surveillance efforts in NATO missions in order to enhance timely detection of biological exposures. As part of those efforts, she is also a member of NATO's STO panel on Pre-Symptomatic Detection of Biological Exposure. Linda also has experience in forensic sciences as an intern at International Criminal Court and from her undergraduate studies at University of Derby and The University of Sheffield. She also contributes to expert discussions surrounding Hybrid CBRN Threats within EU initiatives.

# Bibliography


Ahn, A. (2023, July 18). *How Worried Should We Be About Zaporizhzhia?* Retrieved May 17, 2024, from Foreign Policy: https://foreignpolicy.com/2023/07/18/zaporizhzhia-nuclear-power-plant-threat-russia-ukraine-war/

Alkis, A. (2024, April 17). *Russia plans to restart Ukraine's embattled Zaporizhzhia nuclear power plant. That won't make the plant safer.* Retrieved from Bulletin of the Atomic Scientists: https://thebulletin.org/2024/04/russia-plans-to-restart-ukraines-zaporizhzhia-embattled-nuclear-power-plant-that-wont-make-the-plant-safer/

Altman, J. D., Miner, D. S., E., A. A., Nielson, B. U., Rose, A. M., Honton, K., & Poole, B. D. (2023, February 23). Factors Affecting Vaccine Attitudes Influenced by the COVID-19 Pandemic. *Vaccines, 11*(3). Retrieved May 26, 2024, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10057947/

Badshah, N. (2024, April 7). *Russia accused of using chemical gas attacks against Ukrainian soldiers.* Retrieved April 9, 2024, from The Guardian: https://www.theguardian.com/world/2024/apr/06/russia-accused-of-using-chemical-gas-attacks-against-ukrainian-soldiers

Basit, A. (2021, June). Conspiracy Theories and Violent Extremism: Similarities, Difference and the Implications. *Counter Terrorist Trends and Analyses, 13*(3), 1-9. Retrieved May 28, 2024, from https://www.jstor.org/stable/27040260

BBC. (2017, December 19). *Cyber-attack: US and UK blame North Korea for WannaCry.* Retrieved May 2, 2024, from BBC: https://www.bbc.com/news/world-us-canada-42407488

BBC. (2018, October 8). *Russian spy poisoning: What we know so far.* Retrieved May 2, 2024, from BBC: https://www.bbc.com/news/uk-43315636

BBC. (2024, June 04). *Critical incident over London hospital's cyber-attack.* Retrieved June 11, 2024, from BBC: https://www.bbc.com/news/articles/c288n8rkpvno

Bennett, B. W., Choi, K., Jones, G. S., Cha, D.-H., Park, J., Harold, S. W., . . . Kang, Y. (2022). *Characterizing the Risks of North Korean Chemical and Biological Weapons, Electromagnetic Pulse, and Cyber Threats.* Santa Monica, California: RAND Cooperation. Retrieved April 20, 2024, from https://www.rand.org/pubs/research_reports/RRA2026-1.html

Bilal, A. (2024, April 26). *Russia's hybrid war against thr West.* Retrieved from NATO Review: https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html

Boland, M., & US, T. C. (2018, March 14). *What We Know about Novichok, the "Newby" Nerve Agent Linked to Russia*. Retrieved April 10, 2024, from https://www.scientificamerican.com/article/what-we-know-about-novichok-the-newby-nerve-agent-linked-to-russia/

Carl, N. (2023, June). *Pivot of Offense - How Iran is Adapting for Modern Conflict and Warfare.* Retrieved May 23, 2024, from American Enterprise Institute: https://aei.org/wp-content/uploads/2023/05/Pivot-to-Offense-How-Iran-Is-Adapting-for-Modern-Conflict-and-Warfare.pdf?x91208

CEPI (2024). *Disease X - what it is, and what it is not*, *CEPI*. Retrieved October 28,2024. Available at: https://cepi.net/disease-x-what-it-and-what-it-not

CFR.org Editors. (2022, June 28). *North Korea's Military Capabilities.* Retrieved April 15, 2024, from Council on Foreign Relations: https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities

Cordesman, A. H., & Hwang, G. (2020, September 28). *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations.* Retrieved June 24, 2024, from Center for Strategic & International Studies: file:///C:/Users/gogaczp/Downloads/200702_Burke_Chair_Chinese_Chronology.pdf

Council on Foreign Relations. (2006, October 19). *"Dirty Bombs"*. Retrieved June 6, 2024, from Council on Foreign Relations: https://www.cfr.org/backgrounder/dirty-bombs

Cox, D. G., Bruscino, T., & Ryan, A. (2012, Spring). Why Hybrid Warfare is Tactics Not Strategy: A Rejoinder to "Future Threats and Strategic Thinking". *Infinity Journal, 2*(2), 25-29. Retrieved March 8, 2024, from https://www.militarystrategymagazine.com/wp-content/uploads/2019/11/Military_Strategy_Magazine_Volume_2_Issue_2.pdf

Crowther, G. A. (2021). NATO and hybrid warfare - Seeking a concept to describe the challenge from Russia. In N. Nilsson, M. Weissmann, B. Palmertz, & P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 21-35). London: I.B. Tauris.

CSIS. (2021, December 17). *Bad Idea: Winning the Gray Zone*. Retrieved March 25, 2024, from https://www.csis.org/analysis/bad-idea-winning-gray-zone

Dalton, M., Hicks, K. H., Donahoe, M., Sheppard, L., Friend, A. H., Matlaga, M., . . . Kiernan, J. (August 2019). *By Other Means: Part II: Adapting to Compete in the Gray Zone.* Washington DC: CSIS, Rowman & Littlefield. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_II_interior_v8_PAGES.pdf

Debusmann Jr, B. (2023, February 16). *Ohio train derailment: Rail firm pulls out of meeting with residents.* Retrieved May 28, 2024, from BBC: https://www.bbc.com/news/world-us-canada-64659795

Defence Policy and Planning Division. (2019). *Non-binding guidelines for enhanced civil-military cooperation to deal with the consequences of large-scale CBRN events associated with terrorist attacks.* Retrieved April 4, 2024, from NATO: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/200414-guidelines-civmilcoop-cbrn.pdf

DIA. (2024, February). *IRAN: Enabling Houthi Attacks Across the Middle East.* Retrieved April 23, 2024, from Defense Intelligence Agency: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final2.pdf

DNI. (2024, February 5). *Annual Threat Assessment of the U.S. Intelligence Community.* Retrieved April 12, 2024, from Office of the Director of National Intelligence: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019, February). Understanding Conspiracy Theories. *Advances in Political Psychology, 40*(1), 3-35. doi:doi: 10.1111/pops.12568

Dr Hatchett, R. (2024). *Developing pandemic-busting vaccines in 100 days.* Retrieved June 14, 2024, from CEPI: https://cepi.net/100-days

Dubow, B., Lucas, E., & Morris, J. (2021, Dcember 2). *Jabbed in the Back: Mapping Russian and Chinese Information Operations During the COVID-19 Pandemic.* Retrieved June 3, 2024, from Center for European Policy Analysis: https://cepa.org/comprehensive-

reports/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-the-covid-19-pandemic/

Dupuy, P.-M., & Viñuales, J. E. (2018). *International Environmental Law* (Second Edition ed.). Cambridge: Cambridge University Press. Retrieved March 15, 2024, from https://library.sprep.org/sites/default/files/2021-03/international-environmental-law.pdf

ECHO. (2023, January 17). *resEU: Commission creates first ever chemical, biological, radiological and nuclear strategic reserve in Finland.* Retrieved June 2, 2024, from European Comission - European Civil Protection and Humanitarian Aid Operations: https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/news/resceu-commission-creates-first-ever-chemical-biological-radiological-and-nuclear-strategic-reserve-2023-01-17_en#:~:text=It%20will%20include%20critical%20medical%20countermeasures%2

Ellis-Petersen, H., Lumpur, K., & Haas, B. (2019, April 1). *How North Korea got away with the assassination of Kim Jong-nam.* Retrieved April 17, 2024, from The Guardian: https://www.theguardian.com/world/2019/apr/01/how-north-korea-got-away-with-the-assassination-of-kim-jong-nam

Eurofound. (2022, July 25). *Trust in national institutions is falling: Data behind the decline.* Retrieved June 3, 2024, from European Foundation for the Improvement of Living and Working Conditions: https://www.eurofound.europa.eu/en/blog/2022/trust-national-institutions-falling-data-behind-decline

European Commission. (2016, April 6). *Joint Framework on countering hybrid threats a European Union response.* Retrieved April 1, 2024, from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

European Commission. (2017, October 18). *Action Plan to enhance prepredness against chemical, biological, radiological and nuclear security risks.* Retrieved April 1, 2024, from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0610

European Commission. (2018, June 13). *Increasing Resilience and bolstering capabilities to address hybrid threats.* Retrieved April 1, 2024, from European Union External Action: https://www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

European External Action Service. (2022). *A Strategic Compass for Security and Defence.* Brussels: European Union. Retrieved March 25, 2024, from https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en

European Union External Action. (2024). *Annual Progress Report on the Implementation of the Startegic Compass for Security and Denfence.* Brussels: European Union. Retrieved May 13, 2024, from https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2nd Year_Report_0.pdf

Faulconbridge, G. (2024, March 13). *How many nuclear wpeoans does Russia have and who controls them?* Retrieved April 9, 2024, from Reuters: https://www.reuters.com/world/europe/russias-nuclear-arsenal-how-big-is-it-who-controls-it-2024-03-13/

FBI. (n.d.). *Amerithrax or Anthrax Investigation.* Retrieved June 27, 2024, from Federal Bureau of Investigation: https://www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation

Fildes, J. (2011, February 15). *Stuxnet virus targets and spread revealed.* Retrieved April 11, 2024, from BBC News: https://www.bbc.com/news/technology-12465688

Filipec, O. (2023, September). The Cooperation between EU and NATO in Response to Hybrid Threats - A Retrospective Analysis from the Institutionalist Perspective. *Slovak Journal of Political Sciences, 23*(1), 27-55. Retrieved June 7, 2024, from https://www.researchgate.net/publication/376065756_The_Cooperation_Between_EU_and_NATO_in_Response_to_Hybrid_Threats_A_Retrospective_Analysis_from_the_Institutionalist_Perspective

Fitzgerald, S. (2024, April 24). *Report: Chinese Military Researching Marine Toxins for Bioweapons.* Retrieved June 06, 2024, from Newsmax: https://www.newsmax.com/newsfront/china-military-marine-toxins/2024/04/24/id/1162204/

Fortra. (2015, June 29). *The OPM Breach: Timeline of a Hack.* Retrieved May 2, 2024, from Tripwire Integrity Management: https://www.tripwire.com/state-of-security/the-opm-breach-timeline-of-a-hack

Franke, U. (2023). Drones in Ukraine and beyond: Everything you need to know. *European Council on Foreign Relations*. Retrieved from https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/

Fridman, O. (2019). On the "Gerasimov Doctrine" Why the West Fails to Beat Russia to the Punch. *PRISM, 8*(2), 100-113. Retrieved from https://www.jstor.org/stable/26803233

Fruhlinger, J. (2022, August 31). *Stuxnet explained: The first knoen cyberweapon.* Retrieved April 11, 2024, from CSO: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Galeotti, M. (2014, July 6). *The 'Gerasimov Doctrine' and Russian Non-Linear War.* Retrieved March 14, 2024, from In Moscow's Shadows: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Galeotti, M. (2021, September 29). *Globsec.* Retrieved March 12, 2024, from Thinking about Hybrid War and the 'Imagination Race': https://www.globsec.org/what-we-do/publications/thinking-about-hybrid-war-and-imagination-race

Gardner, H. (2015). Hybrid Warfare: Iranian and Russian Versions of "Little Green Men". In G. Lasconjarias, & J. A. Larsen, *NATO's Response to Hybrid Threats* (pp. 163-188). Rome: NATO Defence College.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats - A conceptual model.* European Commission, Hybrid CoE, Joint Research Centre. Luxemburg: Publications Office of the European Union. doi:10.2760/44985

Giles, K. (2015). Conclusions: Is Hybrid Warfare Really New? In G. Lasconjarias, & J. A. Larsen, *NATO's Response to Hybrid Threats* (pp. 321-337). Rome: NATO Defence College.

Gillard, E.-C. (2020, December 14). *Seventy Years of the Geneva Convention.* Retrieved June 11, 2024, from Chatham House: https://www.chathamhouse.org/2020/03/seventy-years-geneva-conventions/protection-medical-care-armed-conflict

Gorden, J. S. (2017). Intelligence sharing in NATO. *Atlantisch Perspectief, 41*(6), 15-19. Retrieved May 12, 2024, from https://www.jstor.org/stable/48581386

Granholm, F., Tin, D., & Ciottone, G. R. (2023). The Complexities of Hybrid Warfare and the Impact on Tactical Emergency Medical Support. *Health Security, 21*(3), 242-245. doi:10.1089/hs.2022.0161

Harding, L. (2020, June 23). *'A chain of stupidity': the Skripal case and the decline of Russia's spy agencies*. Retrieved April 10, 2024, from

https://www.theguardian.com/world/2020/jun/23/skripal-salisbury-poisoning-decline-of-russia-spy-agencies-gru

Headley, T. (2020, December 3). *How Terrorists Could Use Biological Weapons to Kill Millions.* Retrieved May 6, 2024, from National Interest: https://nationalinterest.org/blog/reboot/how-terrorists-could-use-biological-weapons-kill-millions-173698

Hicks, K. H., Friend, A. H., Federici, J., Shah, H., Donahoe, M., Conklin, M., . . . Sheppard, L. (2019). *By Other Means: Part I: Campaigning in the Gray Zone.* Center For Strategic & International Studies. Washington DC: CSIS, Rowman & Littlefield. Retrieved April 12, 2024, from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf

Higgins, E. (2021, February 4). *How Bellingcat uncovered Russia's secret network of assassins.* Retrieved April 10, 2024, from Wired: https://www.wired.com/story/russia-bellingcat-poison/

Hybrid CoE. (2019, October). *Nuclear energy and the current security environment in the era of hybrid threats.* e European Centre of Excellence for Countering Hybrid Threats. Helsinki: Hybrid CoE. Retrieved March 8, 2024, from Hybrid CoE: https://www.hybridcoe.fi/publications/nuclear-energy-and-the-current-security-environment-in-the-era-of-hybrid-threats/#:~:text=Nuclear%20energy%20and%20the%20current%20security%20environment%20in,obvious%2C%20but%20hidden%20and%20derive%20from%20spill-ov

Hybrid CoE. (2024). *Hybrid Threats*. Retrieved March 08, 2024, from https://www.hybridcoe.fi/hybrid-threats/

IAEA. (2024). *IAEA Incident and Trafficking Database - 2024 Factsheet.* Retrieved May 15, 2024, from IAEA: https://www.iaea.org/sites/default/files/24/05/itdb_factsheet_2024.pdf

Interpol. (2017). *Public Messages to use in the immediate response to a CBRN Attack*. Retrieved May 15, 2024, from INTERPOL: https://www.interpol.int/content/download/583/file/CBRNE_Messaging%20Guidance_2017_FINAL.pdf

Interpol. (n.d.). *Radiological and Nuclear terrorism*. Retrieved May 15, 2024, from INTERPOL: https://www.interpol.int/en/Crimes/Terrorism/Radiological-and-Nuclear-terrorism#:~:text=The%20threat%20Nuclear%20and%20other%20radiological%20materials%20have,be%20used%20in%20terrorism%20or%20other%20criminal%20acts

Jash, A. (2019). Fight and Win Without Waging a War: How China Fights Hybrid Warfare. *Center for Land Warfare Studies Journal*, 96-109. Retrieved June 24, 2024, from https://www.researchgate.net/profile/Amrita-Jash/publication/339847883_Fight_and_Win_Without_Waging_a_War_How_China_Fights_Hybrid_Warfare/links/5e68f4d94585153fb3d65767/Fight-and-Win-Without-Waging-a-War-How-China-Fights-Hybrid-Warfare.pdf

Johnson, D. (2015). Russia's Approach to Conflict: Implications for NATO's Deterrence and Defence. In G. Lasconjarias, & J. A. Larsen, *NATO's Response to Hybrid Threats* (pp. 137-160). Rome: NATO Defence College.

Johnson, D. (2018, December 20). *VOSTOK 2018: Ten years of Russian strategic exercises and warfare preparations.* Retrieved April 29, 2024, from NATO Review: https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html

Koehler, D. (2019, December). The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. *Combating Terrorism Center at West Point - CTCSentinel,*

*12*(11), pp. 14-20. Retrieved April 20, 2024, from https://ctc.westpoint.edu/wp-content/uploads/2020/02/CTC-SENTINEL-112019.pdf

Kubica, L. (2024, January 29). *Hybrid CoE Working Paper 28: Moldova's struggle against Russia's hybrid threats: from countering the energy leverage to becoming more sovereign overall.* The European Centre of Excellence for Countering Hybrid Threats. Retrieved March 05, 2024, from Hybrid CoE: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/

Kushner, D. (2024, January 19). *The Real Story of Stuxnet.* Retrieved April 11, 2024, from IEEE Spectrum: https://spectrum.ieee.org/the-real-story-of-stuxnet

Landay, J., Psaledakis, D., & Hunnicutt, T. (2024, June 17). *Over 20 NATO allies to sepnd at least 2% of GDP on defense in 2024, says Stoltenberg.* Retrieved June 3, 2024, from Reuters: https://www.reuters.com/world/europe/over-20-nato-allies-spend-least-2-gdp-defense-2024-says-stoltenberg-2024-06-17/

Lasconjarias, G., & Larsen, J. A. (2015). Introduction: A New Way of Warfare. In G. Lasconjarias, & J. A. Larsen, *NATO's Response to Hybrid Threats* (pp. 1-14). Rome: NATO Defence College.

Lee, J., White, G., & Jones, V. (2023, April 1). *Lazarus Heist: The Interncontinental ATM theft that netted $14m in two hours.* Retrieved April 15, 2024, from BBC: https://www.bbc.com/news/world-65130220

Levy, S. B., & Marshall, B. (2004). Antibacterial resistance worldwide: causes, challenges and responses. *nature medicine, 10*(Suppl 12), 122-129. doi:https://doi.org/10.1038/nm1145

Łubiński, P. (2022). Hybrid Warfare or Hybrid Threat - The Weaponization of Migration as an Example of the Use of Lawfare - Case Study of Poland. *Polish Political Science Yearbook, 51*, 1-13. doi:https://doi.org/10.15804/ppsy202209

Madsen, J. M. (2023, January). *Overview of Chemical-Warfare Agents.* Retrieved April 29, 2024, from MSD Manual: https://www.msdmanuals.com/professional/injuries-poisoning/mass-casualty-weapons/overview-of-chemical-warfare-agents

Mason, J., & Holland, S. (2023, June 10). *Russia received hundreds of Iranian drones to attack Ukraine, US says.* Retrieved April 23, 2024, from Reuters: https://www.reuters.com/world/europe/russia-has-received-hundreds-iranian-drones-attack-ukraine-white-house-2023-06-09/

McGruddy, J. (Fall 2013). Multilateral Intelligence Collaboration and International Oversight. *Journal of Strategic Security, 6*(3, Supplement: Ninth Annual IAFIE Conference: Expanding the Frontiers of Intelligence Education), 214-220. Retrieved June 11, 2024, from https://www.jstor.org/stable/26485072

Merrifield, J. S. (2024, March 21). *Climate change is warming public opinion to nuclear power*. Retrieved June 3, 2024, from Financial Times: https://www.ft.com/content/6fe4cb92-d49a-4f71-8633-d6a26a695300

Milne, R. (2024, April 28). *Russian GPS jamming threatens air disaster, warn Baltic ministers.* Retrieved May 3, 2024, from Financial Times: https://www.ft.com/content/37776b16-0b92-4a23-9f90-199d45d955c3

Monaghan, S. (2019). Countering Hybrid Warfare: So What for the Future Joint Force? *PRISM, 8*(2), 82-98. Retrieved March 8, 2024, from https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf

Nadimi, F. (2018, August 16). *Iran's Passive Defense Organization: Another Target for Sanctions.* Retrieved April 16, 2024, from The Washington Institute for Near East Policy: https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions

NATO/OTAN. (2014, September 05). *Wales Summit Declaration*. Retrieved March 21, 2024, from https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO/OTAN. (2022a, June 29). *NATO 2022 Strategic Concept.* Retrieved April 1, 2024, from NATO: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO/OTAN. (2022b, July 05). *NATO's Chemical Biological, Radiological and Nuclear (CBRN) Defence Policy*. Retrieved March 18, 2024, from https://www.nato.int/cps/en/natohq/official_texts_197768.htm

NATO/OTAN. (2023, November 08). *NATO's approach to countering disinformation.* Retrieved May 28, 2024, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_219728.htm

NATO/OTAN. (2024a, March 7). *Countering hybrid threats*. Retrieved March 08, 2024, from https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO/OTAN. (2024b, April 11). *Science for Peace and Security - Key Priorities.* Retrieved June 5, 2024, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/85291.htm

NATO/OTAN. (2024c, April 29). *Science for Peace and Security.* Retrieved June 5, 2024, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/78209.htm

NATO/OTAN. (2024d, May 2). *Statement by the North Atlantic Council on recent Russian hybrid activities.* Retrieved May 6, 2024, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_225230.htm

NATO Standardization Office. (2012, January 30). *Record 16263 "situational awareness"*. Retrieved May 23, 2024, from NATOTerm, the official NATO Terminoligy Database: https://nso.nato.int/natoterm/Web.mvc

NATO Standardization Office. (2022, July 18). *Record 17638 "Intelligence"*. Retrieved May 23, 2024, from NATOTerm the official NATO Terminology Database: https://nso.nato.int/natoterm/Web.mvc

NATO Standardization Office. (2022, January). *AJMedP-7 Allied Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Medical Support Doctrine*. Retrieved June 3, 2024, from https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-7_EDB_V1_E_2596.pdf

NATO Strategic Communications Centre of Excellence. (2020). *About Startegic Communications.* Retrieved May 6, 2024, from NATO Strategic Communications Centre of Excellence: https://stratcomcoe.org/about_us/about-strategic-communications/1#:~:text=What%20is%20NATO%20StratCom%3F,order%20to%20advance%20NATO%27s%20aims.

Newton, S. (2024, June 06). *Qilin: What we know about the Russian gang behind London hospital cyber attack.* Retrieved from Independent: https://www.independent.co.uk/news/uk/home-news/qilin-russia-cyber-gang-london-b2557123.html

Nilsson, N., Weissmann, M., Palmertz, B., Thunholm, P., & Häggström, H. (2021). Security challenges in the grey zone - Hybrid threats and hybrid warfare. In N. Nilsson, M.

Weissmann, B. Palmertz, & P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 1-18). London: I.B. Tauris.

Noga, M., & Jurowski, K. (2023). What do we currently know about Novichoks? The state of the art. *Arch Toxicol, 97*, 651-661. doi:https://doi.org/10.1007%2Fs00204-022-03437-5

NTI. (2024, February 19). *Iran - Country Sportlight.* Retrieved April 15, 2024, from Nuclear Threat Initiative: https://www.nti.org/countries/iran/

Office of the Director of National Intelligence. (2017). *Assessing Russian Activities and Intentions in Recent US Elections.* Office of the Director of National Intelligence. Retrieved April 12, 2024, from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Oliveira, M., Mason-Buck, G., Ballard, D., Branicki, W., & Amorim, A. (2020, September). Biowarfare, bioterrorism and biocrime: A historical overview on microbial harmful applications. *Forensic Science Interntional, 314*. doi:https://doi.org/10.1016/j.forsciint.2020.110366

Pauwels, E. (May 2021). *Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks.* Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats. Retrieved March 10, 2024, from https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210503_Hybrid_CoE_Strategic_Analysis_26_Cyber_biosecurity_WEB.pdf

Parachini, J. V. (2022, September 12). *Debunking Russian Lies About Biolabs at Upcoming U.N. Meetings.* Retrieved June 3, 2024, from RAND Corporation: https://www.rand.org/pubs/commentary/2022/09/debunking-russian-lies-about-biolabs-at-upcoming-un.html

Parsi, R. (2021). Iran's hybrid warfare capabilities. In N. Nilsson, M. Weissmann, B. Palmertz, & P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 232-239). London: I.B. Tauris.

Pifer, S. (2023, October 13). *Russia, nuclear threats, and nuclear signaling.* Retrieved April 9, 2024, from Brookings: https://www.brookings.edu/articles/russia-nuclear-threats-and-nuclear-signaling/

Pummerer, L., Böhm, R., Lilleholt, L., Winter, K., Zettler, I., & Sassenberg, K. (2022, January). Conspiracy Theories and Their Societal Effects During the COVID-19 Pandemic. *Social Psychology and Personality Science, 13*(1), 49-59. doi:10.1177/19485506211000217

Prof Puwal, S. (2024, April 12). *Should aritficial intelligence be banned from nuclear weapons system?* Retrieved April 19, 2024, from NATO Review: https://www.nato.int/docu/review/articles/2024/04/12/should-artificial-intelligence-be-banned-from-nuclear-weapons-systems/index.html?utm_medium=email&utm_campaign=NATO%20Review%20AI%20and%20nuclear%20weapons%20systems&utm_content=NATO%20Review%20AI%20and

Qiu, L. (2022, March 11). *Theory About U.S.-Funded Biowepaons Labs in Ukraine Is Unfounded.* Retrieved May 2, 2024, from The New York Times: https://www.nytimes.com/2022/03/11/us/politics/us-bioweapons-ukraine-misinformation.html

Reddy, D. S. (2024, February). Progress and Challenges in Developing Medical Countermeasures for Chemical, Biological, Radiological, and Nuclear Threat Agents. *The Journal of Pharmacology and Experimental Therapeutics, 388*(2), 260-267. doi:https://dx.doi.org/10.1124/jpet.123.002040

Reflection Group appointed by the NATO Secretary General. (2020, November 25). *NATO 2030: United for a New Era.* Retrieved April 04, 2024, from NATO:

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

Rimpler-Schmid, A., Trapp, R., Leonard, S., Kaunert, C., Dubucq, Y., Lefebvre, C., & Mohn, H. (2021, July 16). *EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats.* Retrieved April 10, 2024, from Think Tank European Parliament: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU(2021)653645_EN.pdf

Rühle, M. (2021). NATO's Response to Hybrid Threats. In D. P. Jankowski, & T. Stępniewski, *NATO in the Era of Unpeace: Defending Aginst Known Unknowns* (pp. 59-80). Brussels-Lublin: Instytut Europy Środkowej / Institute of Central Europe.

Saalman, L. (2021). China and its hybrid warfare spectrum. In N. Nilsson, M. Weissmann, B. Palmertz, & P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 95-112). London: I.B. Tauris.

Schmitt, E. (2016, November 21). *ISIS Used Chemical Arms at Least 52 Times in Syria and Iraq, Report Says.* Retrieved April 12, 2024, from The New York Times: https://www.nytimes.com/2016/11/21/world/middleeast/isis-chemical-weapons-syria-iraq-mosul.html

Schwirtz, M., & Barry, E. (2018, September 9). *A Spy Story: Sergei Skripal was a Little Fish. He had a Big Enemy.* Retrieved April 10, 2024, from https://www.nytimes.com/2018/09/09/world/europe/sergei-skripal-russian-spy-poisoning.html

Seskuria, N. (2021, September 21). *Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools.* Retrieved March 05, 2024, from Center for Strategic & International Studies: https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools

Simpson, E. M. (2005). Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims. *Annual Meeting of the Midwest Political Science Association*, (pp. 7-11). Chicago.

Tagesschau. (2020, October 6). *OPCW bestätigt Fund von Nowitschok.* Retrieved May 2, 2024, from tagesschau.de: https://www.tagesschau.de/eilmeldung/nawalny-opcw-101.html

Tenenbaum, E. (2015). Hybrid Warfare in the Strategic Spectrum: An Historical Assessment. In G. Lasconjarias, & J. A. Larsen, *NATO's Response to Hybrid Threats* (pp. 95-112). Rome: NATO Defence College.

Thurau, J. (2024, January 28). *Deutschland und die Kernenergie: Das Aus ist wohl endgultig*. Retrieved June 3, 2024, from Deutsche Welle: https://www.dw.com/de/deutschland-und-die-kernenergie-das-aus-ist-wohl-endg%C3%BCltig/a-68081277

Tusk, Donald; Juncker, Jean-Claude; Stoltenberg, Jens. (2017, December 05). *Joint Declaration Warsaw 8 July 2016.* Retrieved April 04, 2024, from NATO/OTAN: https://www.nato.int/cps/en/natohq/official_texts_133163.htm

Tzu, S. (2004). *The Art of War.* (L. Giles, Ed.) Project Gutenberg. Retrieved March 19, 2024, from https://ia903407.us.archive.org/35/items/TheArtOfWarBySunTzu/ArtOfWar.pdf

United Nations. (2024, April 15). *Prospect of Nuclear Accident 'Dangerously Close' at Zaporizhzhia Power Plant in Ukraine, International Atomic Energy Agency Chief Warns Security Council.* Retrieved May 17, 2024, from United Nations Meeting Coverage and Press Releases: https://press.un.org/en/2024/sc15662.doc.htm

United Nations Office for Disarmament Affairs Treaties Database. (n.d.). *Treaty on the Prohibtion of Nuclear Weapons*. Retrieved April 19, 2024, from UNODA: https://treaties.unoda.org/t/tpnw/participants

United Nations Office for Disarmament Affairs. (no date). *UN Security Council resolution* 1540 (2004). Retrieved October28, 2024. https://disarmament.unoda.org/wmd/sc1540/

U.S. Department of Defense. (2023). *Military and Security Developments involving the People's Republic of China.* Washington DC: Department of Defense. Retrieved April 15, 2024, from https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

U.S. Department of State. (2023, March 14). *The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons.* Retrieved April 9, 2024, from U.S. Department of State: https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/

Wasser, B., & Matuschak, J. (2022, May 10). *Risk and Responsibility - Managing Future Iranian Weapons of Mass Destruction Threats.* Retrieved April 15, 2024, from Center for a New American Security: https://www.cnas.org/publications/reports/risk-and-responsibility

Weissmann, M. (2021). Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. In N. Nilsson, M. Weissmann, B. Palmertz, & P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 61-82). London: I.B. Tauris.

WHO. (2023, May 30). *WHO records more than 1000 attack on helath care in Ukraine over the past 15 months of full-scale war.* Retrieved June 11, 2024, from World Health Organization: https://www.who.int/europe/news/item/30-05-2023-who-records-1-000th-attack-on-health-care-in-ukraine-over-the-past-15-months-of-full-scale-war

WHO. (2022, July 15). *COVID-19 pandemic fuels largest continues backslide in vaccinations in three decades.* Retrieved May 6, 2024, from World Health Organization: https://www.who.int/news/item/15-07-2022-covid-19-pandemic-fuels-largest-continued-backslide-in-vaccinations-in-three-decades

World Economic Forum. (2024). *The Global Risks Report 2024* (19th Edition ed.). Geneva: World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

# ANNEXES - Interviews

## Interview 1

**25th April 2024, 10:15**

**The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 2

**3rd May 2024, 10:30**

**The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 3

**14th May 2024, 10:00**

**The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 4

**15th May 2024, 10:00**

**The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 5

**29th May 2024, 10:00**

**The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 6

**30st May 2024, 10:30**

**This interview focused on intelligence and information sharing. The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 7

**31st May 2024, 09:00**

**This interview focused on strategic communication. The transcript of this interview is not included in the public release version of this report and will remain in the**

**possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**

## Interview 8

**3rd June 2024, 10:00**

**This interview focused on crisis and risk communication. The transcript of this interview is not included in the public release version of this report and will remain in the possession of the Joint Chemical, Biological, Radiological, and Nuclear Defence Centre of Excellence.**