

CBRN DISINFORMATION – VIEWS FROM EXPERTS

SUMMARY OF FINDINGS



SEPTEMBER 2025

OVERVIEW

The Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP) seeks to understand and counter state-sponsored or state-adjacent disinformation across Chemical, Biological, Radiological, and Nuclear (CBRN) threats. As part of this effort, the Johns Hopkins Center for Health Security (JHCHS) **synthesized expert opinions** on high-level global policy approaches **the diplomatic community could use to manage and counter CBRN disinformation**. JHCHS conducted formal interviews with a broad range of experts and rigorously analyzed their responses to identify themes and recommendations. **Findings underscore the urgent need for tailored countermeasures and enhanced collaboration to implement proactive strategies** like prebunking and amplifying factual information through trusted voices.

METHODOLOGY

We recruited **key informants (KIs) with subject matter expertise in disinformation and/or CBRN weapons** representing government institutions, United Nations (UN) organizations, academic institutions, non-governmental organizations, and think tanks located in the United Kingdom, United States of America (US), Canada, Ukraine, Norway, Sweden, Austria, Finland, Italy, and Belgium. Those who agreed to participate took part in a 45-minute virtual solo or group interview with JHCHS researchers, including at least one lead interviewer and a note-taker. All participants provided consent and all but two provided full permission to record and transcribe the interview. These two interviews were recorded using only audio recordings or notetaking. All interviews followed a semi-structured interview guide, shared with participants in advance via email.

In total, we conducted 24 interviews with 28 experts, who provided insights into the current state of CBRN disinformation, perceived goals and recommendations to guide future countermeasures. To systematically identify impacts and themes, we developed a qualitative analysis codebook and used it to conduct a thematic analysis of transcripts. To ensure high levels of reliability, all transcripts were reviewed by all members of the research team and were each coded independently by two trained coders, who used a process of negotiated agreement to settle differences.

FINDINGS

Interviews with experts revealed deep concern about the growing impact of disinformation on CBRN threats, particularly during acute crises like Russia's invasion of Ukraine. KIs noted that **CBRN-related disinformation targets diverse audiences**, ranging from specific geographic communities (domestic Russian populations, communities where biolabs are located, etc.), to government officials, to society at large. KIs also noted that disinformation is spread through various mechanisms, from simple social media posts to official multilateral forums such as meetings of the Biological Weapons Convention (BWC). KIs described multifaceted goals of disinformation, including **eroding the credibility of adversaries, undermining multilateral institutions, and justifying military actions**. These narratives often **create "infodemic" conditions**, leading to confusion, wasted resources, and compromised trust and transparency. To counter this threat, KIs recommended **proactive strategies** like **prebunking** and **amplifying factual information through trusted voices**, alongside **strengthening the technical authority** of multilateral organizations. These findings underscore the urgent need for **tailored countermeasures and enhanced collaboration** between governments, experts, and technology platforms to build resilience against this evolving threat.

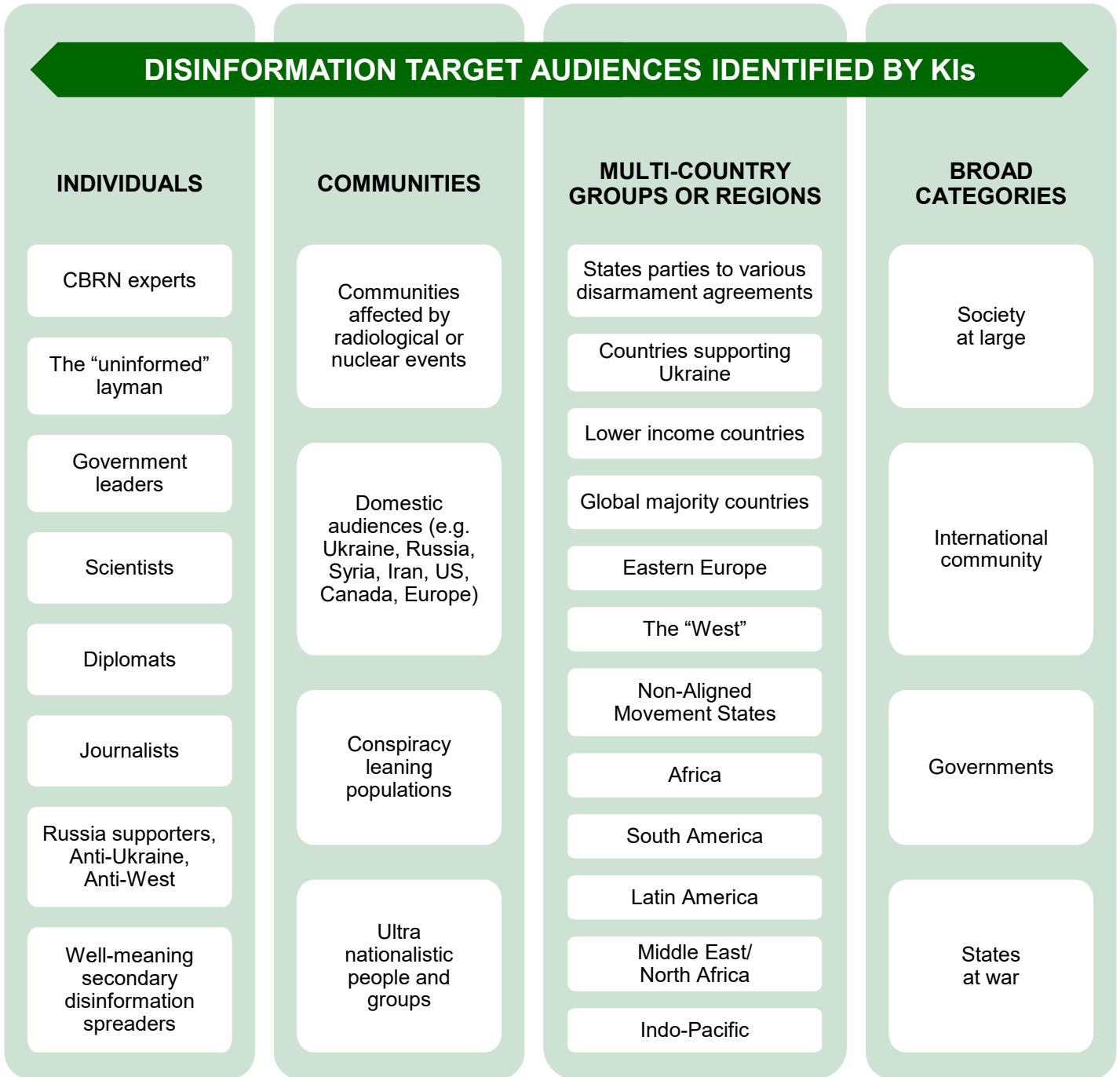
Experts noted that **disinformation tactics and themes often differ between CBRN categories, though the overall purpose of distraction and confusion remains consistent**. Themes from this analysis align with tactics characterized in our taxonomy of CBRN disinformation in pro-Kremlin news media; our [Tactic Spotlight briefs](#) describe these tactics, as well as the overarching master narratives they employ.

Scan this QR code to read more about common CBRN disinformation tactics



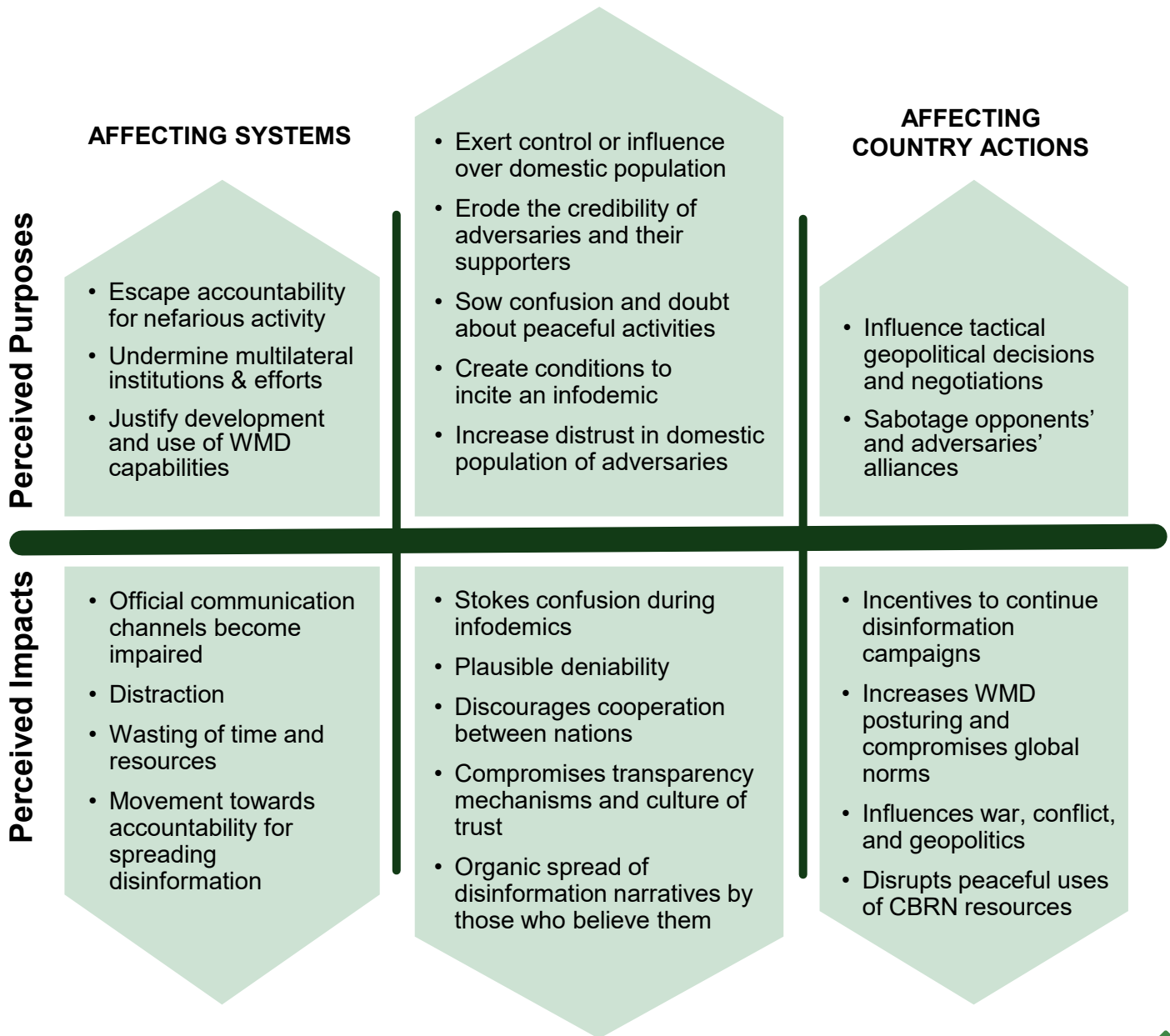
| THEME | DESCRIPTION |
|---|--|
| DISTRACTION & MISDIRECTION | Pointing to (real or falsely alleged) CBRN activity and threats, such as weapons use, attacks on facilities, or emerging dangers. This approach is designed to cause confusion about what may be happening on the ground, justify potential use of weapons, and/or direct attention away from potentially embarrassing events or a country's own CBRN activities. |
| DISCREDITING OPPONENTS | Using disinformation to discredit opponents in the eyes of the international community and/or the disinformation spreader's domestic population. This includes portraying states and entities (including foreign aid initiatives) as "puppets" of a foreign power. |
| USE OF MISLEADING "EVIDENCE" | Referencing, describing, or alluding to "evidence" that purportedly confirms false claims about CBRN weapons/threats. Such evidence may include agreements, documents, reports, and other "materials." In some cases, these materials are legitimate but are deliberately misinterpreted or taken out of context. In other cases, these materials are partially or fully fabricated. |
| FRAMING RUSSIA AS A SAVIOR | Framing Russian actions as necessary to ensure global peace and security. By drawing attention to alleged CBRN and other security threats that purportedly require Russian intervention, this tactic is designed to legitimize Russia as a responsible international actor and justify its aggression in Ukraine. |
| USING "AUTHORITATIVE" SOURCES | Referencing "authoritative" sources to provide a false appearance of legitimacy or expert backing. These sources may be fake, taken out of context, paid by/ part of the originator of the disinformation, or have expertise in a separate area. |
| REFERENCES TO PAST OR PRESENT CRISES | Linking current CBRN threats (real or falsely alleged) with historical disasters or atrocities such as genocide, the Chernobyl disaster, or the Holocaust to evoke a strong emotional response. |
| DISREGARD FOR RULES & NORMS | Falsely alleging that a country or entity is disregarding or breaking rules, laws and norms to discredit opponents. |
| RISK INCREASING LANGUAGE | Narratives with risk increasing language as a psychological tactic to increase fear and/or serve as a threat. |
| CLAIMS OF VICTIMIZATION | Framing the disinformation spreader as victim of real or perceived wrongdoings to distract from or minimize the harms committed by the supposed "victim." |
| TAILORING | Tailoring disinformation to audience preferences for how they receive information or what sources they trust to increase the uptake and effectiveness of disinformation. |

KIs described a range of potential target audiences for CBRN-related disinformation, listing entities as specific as “communities affected by [past] radiological or nuclear events” and as broad as “society at large”. KIs noted that disinformation is **spread across a variety of channels and platforms**, including social media, news outlets, press conferences, online forums, schoolbooks, seemingly legitimate convenings where disinformation can be spread strategically, official multilateral fora, bots and troll farms, Artificial Intelligence (AI)-driven channels, and deepfake videos. In some cases, KIs were even more specific, citing **networks and media spaces in Ukraine that were allegedly owned by Russian media groups**. KIs also highlighted that there was often **secondary proliferation of disinformation** where existing disinformation was leveraged and further propagated by groups and individuals aligned with those who created the initial false messages. The figure below shows the different types of target audiences.

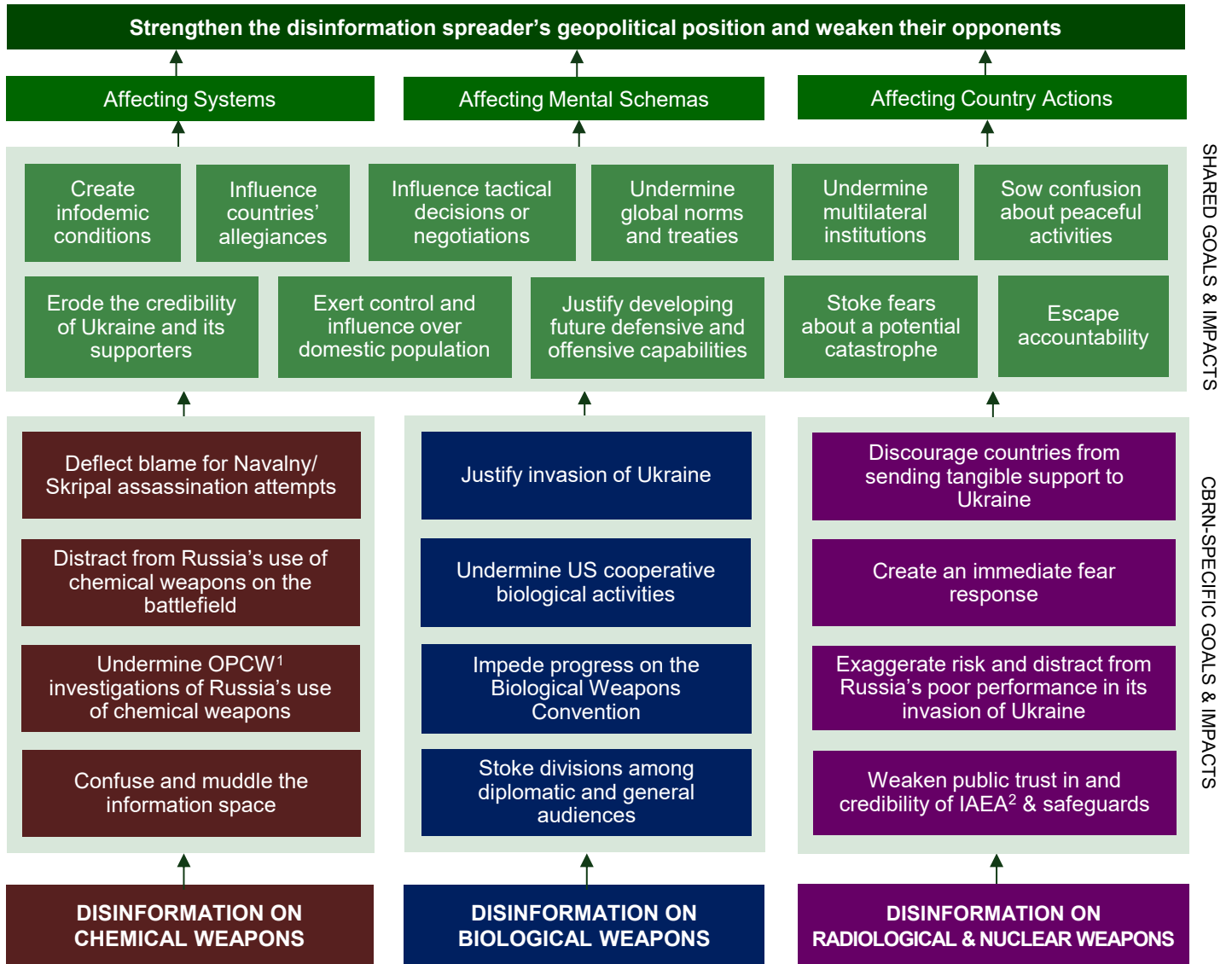


KIs shared that CBRN disinformation seemed to **work towards potential goals** and was **spread for specific purposes**. These perceived goals and purposes can be categorized across three broad categories: impacts to mental schemas, impacts to systems, and impacts to country-level activities. **“Affecting mental schemas”** refers to the cognitive and psychological angles of disinformation, such as attempts at targeting emotions and changing people’s opinions. **“Affecting systems”** encompasses the process of disrupting decision-making, proceedings, and action at the institutional and multilateral levels. It can include attempts to undermine disarmament agreements, while also encompassing efforts to influence entire sectors, such as advancements in technology and communication. **“Affecting actions”** at the country level includes the influence of inter and intra-country policy and law. These categories are not mutually exclusive; rather, they interact dynamically. For example, efforts to reduce the morale of Ukrainian citizens (affecting mental schemas) can, in turn, undermine the broader effort countering Russia’s full-scale invasion of Ukraine (affecting country actions). The figure below shows more examples of perceived goals and impacts across these three categories.

AFFECTING MENTAL SCHEMAS



KIs shared that the **goals and impacts of CBRN disinformation campaigns seemed to differ based on the type of threat**. For example, participants felt that disinformation on chemical weapons created confusion and muddled the information space, while disinformation on radiological and nuclear weapons evoked a strong sense of fear due to the high-risk perception of nuclear threats. However, **several common goals and impacts were identified that spanned all threats**, including inviting suspicion of Ukraine’s credibility and undermining global nonproliferation norms. Almost all disinformation claims seemed to target **two higher-order goals**: improving how the world perceived the disinformation spreader and weakening or undermining the spreader’s opponents. **Goals also could be separated by their effect on systems, mental schemas, and country actions**. These threat-specific and threat-agnostic goals and impacts are illustrated below:



NOTE: This is not an exhaustive list and represents only perceived or suspected (not confirmed) goals and impacts.

CBRN disinformation has tangible impacts like **eroding public trust in institutions** that safeguard against CBRN threats, **influencing domestic and international perspectives** on the actions of nation states, and **overwhelming people with a ‘firehose of falsehoods’** that may keep them from verifying facts. KIs suggested that disinformation **impacts diplomatic spaces**, weakening the nonproliferation, arms control, and disarmament (NACD) architecture over time and often distracting from important international action on other time-sensitive threats.

¹ Organisation for the Prohibition of Chemical Weapons ² International Atomic Energy Agency



The below figure illustrates factors that facilitate disinformation, as well as proposed recommendations to counter CBRN disinformation across multiple levels, based on our discussions with KIs.

| | DISINFORMATION FACILITATORS | KI RECOMMENDATIONS TO COUNTER DISINFORMATION |
|--------------|--|--|
| INSTITUTIONS | <ul style="list-style-type: none"> ▪ Lack of time/resources to identify and counter disinformation ▪ Siloed knowledge and countermeasures due to the discrete and distinct ways in which chemical, biological, and/or nuclear threat reduction and policymaking occurs ▪ Weakening of CBRN disarmament structures ▪ Lack of monitoring and regulation on social media ▪ Emerging technology such as AI and novel WMD technologies | <ul style="list-style-type: none"> ▪ Bolster media literacy to build public resilience to disinformation ▪ Dedicate resources to tracking and analyzing disinformation ▪ Increase funding for research on successfully and effectively countering CBRN disinformation ▪ Enhance disarmament expertise by ensuring fact checkers have sufficient WMD-related knowledge and creating more opportunities for experts to provide input in various decision-making fora ▪ Promote open-source verification tools (e.g., satellite imagery) and encourage their use by non-governmental organizations ▪ Encourage institutions to proactively counter disinformation ▪ Collaborate with technology companies to counter disinformation ▪ Promote stronger accountability measures against disinformation in multilateral fora ▪ Implement cyber countermeasures against and expose verified disinformation sources |
| COMMUNITY | <ul style="list-style-type: none"> ▪ Past grievances and crises ▪ Geopolitical tensions ▪ Emergencies that increase vulnerability to disinformation | <ul style="list-style-type: none"> ▪ Tailor communication by adapting messaging to target audiences ▪ Train diplomats to recognize and counter common disinformation narratives related to disarmament ▪ Foster collaborations with public and private organizations ▪ When called upon, support other entities in countering disinformation, particularly if they lack adequate resources to do so |
| INDIVIDUAL | <ul style="list-style-type: none"> ▪ Mistrust in science and institutions ▪ Deception is becoming normalized ▪ WMDs are inherently scary ▪ Lack of knowledge regarding CBRN realities | <ul style="list-style-type: none"> ▪ Invest in information literacy campaigns on disarmament topics ▪ Use prebunking to inoculate people against disinformation ▪ Consider alternative strategies for de-escalation, such as using humor or memes, to reduce the fear and impact of disinformation ▪ Acknowledge the emotional impact of WMD-related disinformation |
| INFORMATION | <ul style="list-style-type: none"> ▪ Lack of trusted voices to debunk ▪ Difficulty discerning what is true ▪ Confusion between disinformation, posturing, and propaganda ▪ Classified nature of CBRN information ▪ Complexity of WMD technology | <ul style="list-style-type: none"> ▪ Amplify factual information using official diplomatic channels, multilateral organizations, and trusted media ▪ Leverage eyewitnesses to effectively debunk false claims about CBRN WMD ▪ Provide adequate context when debunking, including when explaining regulations and dual-use science |

This study both corroborates and extends the existing knowledge regarding disinformation, highlighting unique features and challenges in the disarmament context. Findings underscore the **need for tailored countermeasures at various levels** (institutions, community, individual, and information) that consider the specificities of disarmament fora, the evolving tactics of state actors, and the complex interplay between audiences, information, belief, and behavior. These measures will **require a collaborative approach** at the bilateral and multilateral levels to combat disinformation campaigns as they arise, **improve trust and transparency** between nations, and **bolster global disarmament norms**.