Information Pollution and What It Means for Arms Control

Joseph Rodgers

Introduction

Over the past decade, Russia has stepped up its disinformation campaigns to erode trust in arms control across the nuclear, chemical, and biological domains. The new era of rapidly disseminated disinformation poses significant challenges to U.S. national security and, more specifically, to arms control verification and compliance. In this polluted information environment, offense is king. This paper examines how the Douma chemical weapons attack eroded the Chemical Weapons Convention, how Russian disinformation about fake Ukrainian biological weapons laboratories undermined trust in the Biological Weapons Convention (BWC), and how Russian disinformation campaigns influenced the collapse of the Intermediate-Range Nuclear Forces (INF) Treaty. In each of these cases, Russia used diverse tactics and messaging methods—including social media, news media, and diplomatic channels—to spread false information and create political pressures. These campaigns matter for future U.S. arms control efforts because arms control agreements are inherently political tools susceptible to being undermined by political pressures.

Russian disinformation campaigns have served as a low-cost tactic for Moscow to spread confusion and distrust in the United States and other Western democracies. While these disinformation campaigns have proven effective, they are often rather crudely constructed. Russia often spreads myriad narratives to see which falsehoods stick, an approach Christopher Paul and Miriam Matthews at RAND have dubbed the “firehose of falsehood.” In the three disinformation campaigns discussed here, the spread of Russian propaganda was aided by friendly countries such as China, Syria, and Iran.

It is easier to spread significant amounts of mis- and disinformation than it is to try to counter false information. This challenge is particularly difficult for the U.S. government because public trust in
large institutions has declined nearly everywhere across the board, including in large news media. Americans’ public trust in government has hovered below 20 percent for the past 12 years. This contested information environment has largely lacked a credible verifier of last resort.

It is easier to spread significant amounts of mis- and disinformation than it is to try to counter false information.

It is difficult to accurately assess causality and the impact that disinformation campaigns have, particularly in arms control. Disinformation that goes viral or reaches many people does not necessarily mean there will be tangible ramifications or changes in policy. In each of the three following case studies, Russia’s goals, tactics, and audience changed. Nevertheless, as the U.S. security policy community shifts toward viewing the world as multipolar and dominated by rivalry among three near-peer adversaries, further Russian disinformation will shape the contours of geopolitical competition.

Case Studies

DOUMA AND SOCIAL MEDIA SUBTERFUGE
On April 7, 2018, the Syrian military conducted two chemical weapons attacks in Douma, Syria. The first allegedly occurred at approximately 4:00 p.m., with the second at approximately 7:30 p.m. In both attacks, a gas cylinder was dropped into residential areas, one hitting the roof terrace in a residential neighborhood and the second crashing into an apartment, and reports of the smell of chlorine immediately followed impact. While the exact number of deaths is debated, the bombings killed between 40 and 70 people, with hundreds more treated for chemical-related injuries. Initial media coverage and victim reports included conflicting information on what chemical was in the cylinders—chlorine, sarin, or a mix of both—but the final report from the Organization for the Prohibition of Chemical Weapons (OPCW) only found evidence of chlorine at the sites.

In response to the attack, Israel launched an airstrike on a Syrian air base on April 9, 2018. The United States, United Kingdom, and France also responded with a joint strike on April 14, 2018, destroying a scientific research facility in Damascus, a chemical weapons storage facility west of Homs, and a chemical weapons equipment storage site and important command post near Homs. In addition, the United Kingdom called for the OPCW to host a special session of the Conference of the States Parties to the Chemical Weapons Convention (CWC) regarding the alleged chemical weapons use in Syria and the attempted poisoning of Sergei and Yulia Skripal with a chemical weapons agent in the United Kingdom on June 26–27, 2018. The purpose of the special session was to approve a chemical weapons attribution mechanism under the auspices of the OPCW. Ultimately, 82 members voted to establish this investigation and identification team, and 24 (including Russia, China, and Syria) voted against it.

Immediately following the use of chemical weapons in Douma, a widespread disinformation campaign was launched to deny the occurrence of the attack. This large-scale, persistent disinformation campaign was initially pushed out through official Russian and Syrian Twitter accounts and state-backed media outlets. The seemingly state-directed campaign attempted to flood the information zone with conflicting and contradictory theories and narratives about the attacks in Douma. Overall, the initial disinformation campaign had little impact on public discourse, as mainstream media outlets dominated
the information space with coverage of the attack and international response. However, disinformation took over the narrative on Douma after these outlets turned to other news in the following weeks.

Unlike mainstream media outlets, the digital platforms spreading disinformation continued to discuss the attacks past the initial week. According to a study by the Atlantic Council, from April 10 to 16, 2018, “six of the ten most-retweeted posts [about Douma] came from Assad supporters, out of a total 487,000 posts,” suggesting that disinformation dominated conversations on the topic. The number of retweets of and interactions with disinformation related to Douma was aided by networks of synthetic actors, such as trolls, bots, and cyborgs.

A study by the Center for Nonproliferation Studies found that in the wake of the attacks, networks of synthetic actors in Syria, Russia, and Iran were activated to push narratives meant to defame the OPCW and White Helmets (a humanitarian organization that tracks and assists Syrian communities affected by chemical weapons attacks), discredit claims of Syrian chemical weapons use, suggest jihadists were responsible for the attacks, hint at nuclear escalation in response to Western retaliatory strikes, and “prey on Western religious and cultural sympathies.” This initial disinformation push also coincided with efforts to delay access to the sites by the OPCW fact-finding mission, which arrived in Douma on April 14, 2018.

One week after the attack, the digital disinformation morphed into a complex and hybridized campaign, linking online activists and propaganda blogs via social media. Counternarratives regarding Douma moved quickly beyond propaganda websites with manipulated journalistic content to spread through a network of online activists and journalists with a track record of opposing “Western interventionist” policies and international institutions. This resulted in a new wave of disinformation in which experts from prominent universities or former military officials further pushed disinformation on Douma, often tying the counternarratives in with other conspiracy theories. Digital disinformation was also promoted by more mainstream influencers—such as actress Susan Sarandon, MIT professor Dr. Theodore Postol, and then-presidential candidate Tulsi Gabbard—proving recognizable voices can become enablers of false and misleading narratives.

In addition, the Douma incident serves as an interesting case study of digital disinformation due to two information “leaks” at the OPCW following the publication of official findings. The OPCW's final report was published on March 1, 2019, nearly one year after the attack, declaring evidence of the use of chlorine but no evidence of nerve agents. While the report was met with pushback from Syrian and Russian supporters, the results did not gain significant traction in public discourse—that is, until October 2019, when WikiLeaks published unauthorized reports by two “whistleblowers” who disputed the OPCW's official findings. An independent investigation ensued, concluding the whistleblowers misrepresented their connections to the OPCW and the Douma investigations team and committed a serious, deliberate, and premeditated breach of confidentiality. The OPCW stood by its findings, but the damage was done; declarations of a coverup made their way into mainstream media.

Russian disinformation had an advantage in the Douma case, as it was able to spread quickly by tapping into existing conspiracy theories that further muddied the information space. The interaction of disinformation across social media platforms and personal blogs allowed the disinformation to reach wider audiences—and reach them more quickly than the United States and OPCW could counter the
narratives. The OPCW took one year to publish a final report of findings on the attacks in Douma, leaving the information space open to disinformation and manipulation in the meantime.

Despite this, open-source intelligence (OSINT) investigations by nongovernmental organizations played an important role in countering disinformation while the OPCW conducted its investigation. OSINT investigators at Bellingcat were able to use photos and videos on social media to piece together the timeline of the attack, geolocate roughly where the attacks took place, estimate the number of victims, and tentatively determine that the attack was the result of a gas cylinder most likely filled with chlorine gas dropped from a Mi-8 Hip helicopter originating from Dumayr Airbase in Syria. Similarly, on June 24, 2018, two months after the attack, the New York Times published an augmented-reality visual investigation of the Douma attacks using images and videos found on social media. These OSINT publications provided a factual and credible source to which policymakers could point during their attempts to counter disinformation.

**UKRAINIAN BIOLABS AND THE IMPORTANCE OF EXPERT MESSENGERS**

Prior to invading Ukraine, Russia carried out a sustained disinformation campaign to justify military intervention. From October 2021 to December 2022, disinformation claimed that the United States was developing biological weapons in Ukrainian laboratories to use against Russia. During the Ukraine “biolabs” campaign, Moscow leveraged international partnerships with China to spread these accusations. For example, Lieutenant-General Igor Kirillov (chief of the Nuclear, Biological, and Chemical Protection Troops of the Russian Armed Forces) asserted in March 2022, “We can say with a high probability that one of the goals of the United States and its allies is the creation of bioagents capable to selectively infect various ethnic groups.” The U.S. Defense Threat Reduction Agency’s (DTRA) Biological Threat Reduction Program does invest in biological research at several laboratories in Ukraine. However, this research does not develop biological weapons but rather aids in manufacturing medical countermeasures and enhancing biosafety, biosecurity, and biosurveillance.

The origins of these Russian allegations began long before the war in Ukraine. However, in the run-up to the war, Russia began recirculating disinformation about fake U.S. biological weapons laboratories. On October 7, 2021, the Russian and Chinese ministers of foreign affairs expressed “serious concerns” about the United States’ “military biological activities” in a joint statement at the UN General Assembly regarding the BWC. On February 4, 2022, Russian president Vladimir Putin and Chinese president Xi Jinping reiterated this stance in a joint statement at the winter Olympic games, emphasizing that “domestic and foreign bioweapons activities by the United States and its allies raise serious concerns and questions for the international community regarding their compliance with the BWC.” Three weeks later, Russia invaded Ukraine and further promoted disinformation about Ukrainian biolabs to justify the invasion.

The disinformation about alleged U.S. biological weapons laboratories was further spread by American right-wing pundits such as Tucker Carlson, Steve Bannon, and Alex Jones. In February and March 2022, the hashtag #biolabs trended across Twitter. In the following months, Russia continued its campaign on the international stage. On April 6, Russia hosted an informal session of the UN Security Council to discuss claims of biolabs. On June 29, Russia called for a formal consultative meeting under Article V of the BWC; the formal consultative process opened on August 26 and closed in September but reached no formal conclusions.
Throughout this process, DTRA responded by putting together fact sheets and YouTube videos. Meanwhile, Russia and China spread disinformation across a wide variety of platforms, including news media, social media, and international forums. China was willing to propagate Russian rumors of U.S. biological weapons labs but was hesitant to claim explicitly that biological labs in Ukraine justified the Russian invasion. These pieces of disinformation were most successful when they were picked up and spread by U.S. domestic audiences, particularly audiences on the far right.

During this disinformation campaign, the United States was placed on the defensive and struggled to respond to Russian lies. Washington worked with partners to provide fact sheets and disseminate accurate information about the nature of U.S. labs overseas. However, these fact sheets were not as effective because they were not spread on social media as widely as the disinformation and because many Americans themselves did not believe them. Additionally, since DTRA was the target of the initial Russian disinformation attacks, the agency’s response was less credible due to the lack of third-party validation by actors with large social influence.

These fact sheets were not as effective because they were not spread on social media as widely as the disinformation and because many Americans themselves did not believe them.

DIPLOMACY AND DISINFORMATION: THE INTERMEDIATE-RANGE NUCLEAR FORCES TREATY
The INF Treaty between the United States and the Soviet Union, and later Russia, entered into force in 1987. The treaty first eliminated existing nuclear and conventional ground-launched cruise missiles (GLCMs) and ground-launched ballistic missiles with an intermediate range—defined in the treaty as 500–5,500 kilometers (310–3,420 miles)—and prohibited both countries from developing new ones. However, in 2013, Washington began to express concerns to Moscow that the Russian Novator 9M729 (SSC-8) missile violated the INF Treaty. Early in 2014, U.S. officials met with NATO's Arms Control, Disarmament and Non-Proliferation Committee in Brussels to inform the committee of Russia's confirmed tests of a GLCM of intermediate range, to which Russia responded that U.S. violations were “a lot more numerous.” In July, the U.S. Department of State’s annual Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments report stated the United States had determined Russia was in violation of its obligations under the INF Treaty. The United States continued to raise concerns over Russian noncompliance throughout 2014 and 2015, including at the 2014 Wales NATO summit, at the 2015 Review Conference for the Non-Proliferation Treaty (NPT), in the Department of State’s 2015 report on arms control compliance, and at a press conference at NATO Allied Command in June 2015. Russia’s response to the allegations was to deflect, stating that the U.S. Aegis Combat System installed in Romania was not in compliance with the treaty.

A 2016 report in the New York Times cited anonymous U.S. officials who raised concerns that a new Russian program to field GLCMs violated the INF Treaty. As a result, in November 2016 the United States called for a special verification commission—which included representatives from Belarus, Kazakhstan, Russia, and Ukraine—to address Russia’s alleged noncompliance, though this commission soon stalled. In 2017, although it acknowledged the existence of the SSC-8 GLCM missile, Russia
claimed this was not capable of intermediate ranges. At the same time, the North Atlantic Council found the United States to be in compliance with the INF Treaty; the council also identified a Russian “missile system that raises serious concerns” and called on Moscow “to address these concerns. . . and actively engage in a technical dialogue with the United States.” Yet by October 2018, the United States announced intent to unilaterally withdraw from the treaty due to Russia’s noncompliance, giving Moscow a 60-day ultimatum in December 2018 to rectify the issue. NATO’s foreign ministers also formally declared Russia to be in material breach of the INF Treaty. Absent a response, the United States withdrew from the treaty on August 2, 2019, at which point Russia confirmed it was “formally dead.”

Throughout this period, Russian diplomats used disinformation to deflect and distort the narrative about the INF Treaty. First, they denied the existence of the SSC-8 missile until the United States publicly released information about the new Russian missile. At that time, Russian officials claimed the missile was INF-compliant and that it was the United States, not Russia, that was avoiding discussing the missile. Russian counternarratives centered on claims that the United States was violating the INF Treaty and was solely responsible for its collapse. The Russian Security Council’s deputy secretary, Alexander Venediktov, alleged that the treaty was “unilaterally terminated by the United States, which wanted to remove any legal obstacles to the development of strike weapons.” Russian foreign minister Sergei Lavrov also claimed that the United States was no longer a trustworthy arms control partner, stating, “The Americans’ recent actions suggest an idea that they would be glad to wreck the entire system of international treaties, at least in the sphere of strategic stability and arms control.” Russian officials continued to deny accusations of INF noncompliance as late as December 2022. Overall, disinformation was deployed through Russian officials in meetings and through Russian state-backed media outlets, such as Russian news agency TASS.

Although Russia did not deploy high-tech disinformation tactics regarding its missiles, as it did in the Douma and BWC cases, Russian officials’ public statements and state-backed media articles seemed to aim at providing counternarratives to confuse the public. Additionally, Russia’s noncompliance with the INF Treaty was initially difficult for the United States to prove to allies and partners due to the sensitivity of the arms control verification through national technical means (NTM). Moscow frequently stated that because the United States did not provide proof of the alleged violation, Russia was, in fact, in compliance. A concrete public explanation of the Russian violation was not released by the United States until November 2018, when Director of National Intelligence Dan Coats conducted a press briefing. This delay afforded an offensive advantage to Russia, which was able to use disinformation campaigns to drive the narrative by providing far more details and specifics than the United States and to do so in a succinct way. The United States also struggled to prove its accusations without revealing methods and sources for intelligence gathering. Moreover, the technical nature of the violation—regarding what counts as a “ground-launched” missile—was difficult for the public to understand, enabling Russia to sensationalize reports that the United States was trying to undermine strategic stability. Overall, the INF case shows how disinformation can set the narrative regarding noncompliance in arms control, especially when classified sources are used for verification.

**Implications**

These studies point to four important findings. First, offense has the advantage when it comes to disinformation. Russia often pushes dozens of narratives in its campaigns. Once one narrative
resonates, Russia doubles down on that message. This means that offensive disinformation campaigns can morph and come from many different angles, whereas U.S. attempts to combat disinformation have required sticking to factual accounting, truth, and going on the defensive. Efforts to counter false narratives with fact sheets or press statements also either fail to receive the significant amounts of public attention that disinformation does or are not viewed as credible and trustworthy.

Second, across all three case studies, Russian disinformation was most successful when it was picked up and recirculated by domestic U.S. audiences. In the case of Douma, mainstream influencers and experts from prominent universities unknowingly peddled lies about who was behind Syrian chemical weapons attacks. In the biolabs case, Russian disinformation was spread by conservative U.S. media, including Fox News. The implication is that the impacts of Russian disinformation are significantly magnified when narratives are picked up by influential audiences in the United States.

Third, open-source investigations are vital in defending against disinformation. Russian disinformation about Douma was successfully countered in part through the emerging network of OSINT analysts in civil society. The OSINT community used satellite images to verify chemical weapons use and conduct interviews with Syrian victims, greatly discrediting the Russian and Syrian government narrative.

While public trust in government and major institutions in the United States is declining, OSINT may help fill a vital role as a verifier of valid information.

While public trust in government and major institutions in the United States is declining, OSINT may help fill a vital role as a verifier of valid information.

Finally, the case studies indicate a series of challenges for the future of arms control negotiations, verification, and compliance. Disinformation creates a polluted information ecosystem that problematizes attempts to prove compliance or noncompliance—and undermines the core principle of transparency by creating false narratives and undermining the authority of the targeted actor.

**Recommendations**

In response to the rise in disinformation about arms control institutions and regimes, the United States will need to develop strategies to counter disinformation when it occurs and build overall resilience to disinformation over the longer term. U.S. arms control negotiators, lawyers, inspectors, and policymakers should prioritize ensuring disinformation efforts do not undermine the transparency and confidence-building measures provided by arms control while also enabling effective U.S. verification.

- **“Defend forward” on disinformation.** Today, the United States does not have a coherent counter-disinformation strategy in place. Instead, it has adopted a series of ad hoc approaches in response, often leaving it on the back foot. In the future, the United States should adopt a “defend forward” mindset for disinformation, taking a preemptive as opposed to a reactive stance. This includes taking persistent and proactive measures to disrupt or halt malicious disinformation while also focusing on defending critical infrastructure.

- **Encourage flexible responses by streamlining declassification.** Disinformation campaigns are much more difficult to counter when the truth is veiled in classification and secrecy. In the
case of the INF Treaty, a lack of publicly available information about the nature of Russian violations complicated U.S. assertions. Conversely, U.S. fact sheets responding to Russian biolabs disinformation alleging violations of the BWC empowered fact-based counterarguments. The U.S. government should encourage flexible declassification—in cases where it would not harm national security—to arm the public with intelligence that can be used to counter future disinformation campaigns. Much of the intelligence that the United States collects can be declassified without revealing sources and methods. The Biden administration effectively utilized this tactic in the lead-up to the Russian invasion of Ukraine by declassifying evidence about Moscow’s plans and cyberattacks in Ukraine.

- **Create counter-disinformation measures within arms control treaties.** Disinformation will become a more common tool for adversaries to cause confusion on arms control compliance and verification measures. Future arms control agreements, both formal and informal, should include measures to address and counter any disinformation related to the treaty. This could be done as a consultative commission or as part of compliance and verification. Such mechanisms would require states parties to an agreement to raise concerns of disinformation about the treaty within the commission or through outlined channels—and claims made outside of the official mechanism could be considered a violation of compliance.

- **Establish a role for OSINT in the arms control process.** OSINT has played a crucial role in countering disinformation in all three arms control challenges discussed above. The U.S. government should consider how to bolster the capacity of OSINT organizations in this role. Support for OSINT efforts could include more government sponsorship of open-source intelligence collection and public training sessions on how to conduct OSINT and counter disinformation.

Disinformation campaigns surrounding chemical weapons use in Syria, biological weapons laboratories in Ukraine, and INF Treaty violations have already affected arms control agreements. Russian disinformation campaigns have sought to justify arms control violations and undermine global norms against the use of weapons of mass destruction. These challenges will only be exacerbated by new and emerging technologies. Artificial general intelligence (AGI) such as ChatGPT will enable disinformation campaigns to easily draft hundreds of fictitious narratives to spread on social media; deep fakes of political leaders already have the potential to exacerbate political crises; and decentralized and new forms of social media may become increasingly difficult to regulate, making it more challenging to flag and attribute disinformation. All these emerging and present challenges have serious implications for arms control negotiations and implementation. The time is now to begin thinking about how to defend forward against arms control disinformation.

**Joseph Rodgers** is associate fellow and associate director of the Project on Nuclear Issues at the Center for Strategic and International Studies in Washington, D.C.

The author would like to thank Suzanne Claeys for her contributions to the ideas and recommendations to this report in previous editions of the text.