Keynote Address by Sarah Jacobs Gamberini at The Center for the Study of Democracy Conference on Countering WMD Hybrid Threats and Malign Interference in the Black Sea Region

---

Introduction

Today I have been invited to talk about the security challenge posed by disinformation, to discuss how it is employed strategically, especially connected to topics of chemical, biological, and nuclear weapons. And importantly, how we as democracies can counter this ever-present threat.

Russia's Disinformation Ways and Means

False information pervades our world, and we find that technical areas of science, health and Weapons of Mass Destruction are particularly susceptible to disinformation because of the complexity and inherent fear associated with these topics—where the average public has less expertise and is likely to believe a simple, false story, over the complicated technical truth.

Countries like Russia have used this type of influence to challenge NATO in the information domain, weakening our democratic societies, and undermining faith in our institutions.

To begin, it is important that we speak clearly and have a shared language to refer to the spectrum of false and manipulated content online, and the terms we use to talk about the information environment are too often used interchangeably but they have different methods and different solutions sets.

Misinformation: inadvertent spreading of false content (in this case people sharing false information believe it is true and heard it somewhere and are spreading the message).
Disinformation: malicious and intentional development and propagation of false or manipulated information (ex. instigation Bioweapons conspiracy theory).
Finally, a term you may be less familiar to many of you, but is a common means for Russia to manipulation the information environment, is **Malinformation.**
Malinformation is largely built around facts—but taken out of context or otherwise misleading. We have seen real quotes from our leaders, placed into a malign context that throws doubt on their intentions.

Russia uses all of these methods of manipulating information from its sharing of flat-out false information and deception, to relying on false information to proliferate organically as **misinformation** once a falsehood is adopted and shared by individuals, to the distortion of actual facts, or half-truths and using that to support a false argument that is harder to debunk. This distortion of facts is common in the complicated world of WMD or arms control or high containment security labs.

This is all part of Russia's cross-domain strategy which includes various malign activities, on multiple planes, below threshold of armed conflict. There are lots of examples of how Russia has done this, little green men in Eastern Ukraine when it annexed Crimea, "unaffiliated" private military groups like the Wagner group, Novichok use, and numerous cyberattacks, and because of the nature of this type of warfare likely many more about which we are unaware.

Because of the deniability that Russia has maintained in each of these cases, attribution and proportionality are thrown into question. Russia integrates all military and non-military devices to achieve its strategic goals, including in the information space.

In 2019, Russian General Valery Gerasimov gave a speech in which he called information technologies one of the most promising types of weapons, and not just to be used against critical information infrastructure, like we think about for cyber-attacks, but against the population of a country, directly influencing the state of a nation's security.

These views predate the information age, but information technologies alarming exacerbate these threats. Russia utilizes the full information ecosystem online to spread its narrative---from conventional Russian news and propaganda like the state-controlled television network RT and Sputnik, to a large numbers of Russian web brigades, troll farms, and automated bots to disseminate propaganda on social media like telegram, VK, and others.

Russia also relies on its platforms on the world stage to spread its falsehoods including through its embassies around the world, statements by the ministry of defense and foreign affairs, and at forums like the United Nations and the Chemical Weapons Convention which they regularly use for political theater.

These entities (both human and automated) are constantly putting out new content and amplifying existing content that is pro-Russian or anti- Russia's opponents.

Russia utilizes information warfare to achieve certain objectives.

- Project image of Russian strength and broadcast Russian agendas to the world

- Divide alliances and undermine confidence in democracy
- Erode trust between citizens and institutions
- Create general distrust over information sources, blurring the line between fact and fiction

In looking at which topics Russia targets (democratic elections, politically divisive issues, long held norms around state sovereignty or WMD use), Russia clearly recognizes how to identify these and other seams and fissures within democratic societies and how best to exploit and amplify these divisions.

WMD Disinformation

WMD has long been a target for Russia to employ disinformation. Nuclear, chemical and biological weapons, by virtue of their special status in the box known as weapons of mass destruction, hold a place of fear and unknown in the minds of the public, and Russia has exploited that fear.

Russia has used disinformation, deflection, and deception on behalf of its Syrian ally in using chemical weapons. Russia also sowed dozens of conflicting narratives following its own uses of the novel chemical weapon Novichok, and it uses coercive influence in its nuclear saber-rattling threats.

The Kremlin has also long used disinformation methods to stoke fears about scientific and medical issues: The biological weapons allegations against Ukraine and its public health laboratories mirror the Kremlin's long held public health disinformation strategies: planting stories during the cold war that AIDS was a US bioweapon, in 2014 that Ebola was a bioweapon, and for the last three years that covid was a bioweapon. And Russia has long made false allegations that Department of Defense Sponsored public health research labs in the Republic of Georgia, Fort Detrick and elsewhere are in fact secret U.S. bioweapons laboratories.

Russia seeks to capitalize on the fear of the public about WMD or about diseases that seems to come out of nowhere and suggest that fear should instead be focused on the US government and its allies.

These old disinformation efforts now benefit from the speed and reach of modern media to rapidly shape and influence both opinions and actions across the globe.

And once again in Ukraine, WMD Disinformation is a key part of Russia's strategy:

The conflicting claims range from the familiar to the more absurd: That Ukraine was seeking to create nuclear or radiological weapons, or that Ukraine planned employ chemical weapons against Russian troops, all the way to the more absurd about Ukraine weaponizing birds for bioweapon delivery or even the creation of super soldiers in Ukrainian labs.

So what is Russia trying to accomplish with these WMD narratives in Ukraine?

- At the **strategic level**, the Russian government employs disinformation to influence the actions, postures, and alignments of state governments. The Kremlin seeks to split alliances and coalitions; seeking to fracture NATO's unity in opposition to its actions.
- **At the tactical level**, Russia is likely seeking to achieve several objectives. First, it uses claims that the US utilizes Ukraine as a staging area for biological and chemical weapons, and claims of horrific and illegal human experimentation to fabricate justifications for the invasion of Ukraine;
- Next, Russia's disinformation claiming that the US is already developing or preparing to utilize these weapons normalizes use of weapons of mass destruction. This undermines arms control regimes and international institutions that monitor or prevent WMD development. This normalization also lays the foundation for the Kremlin to employ chemical or biological weapons in Ukraine potentially—and then accuse Ukraine of being responsible.

Russia sows disinformation, especially about WMD topics to create a fog of war and confusion in what is otherwise a very straightforward issue of a large country illegally invading its smaller neighbor.

One main reason Russia use disinformation is to increase the political cost of foreign partners doing business with the USG. By spreading disinformation in societies, and allowing those narratives to become grassroots and poison the dialogue, it undermines the exercises, activities, and engagement programs between our countries. By raising concerns, or even doubt, about the US intentions in host nation populations, we risk the future of these programs and the important exchange of information that it provides.

Conclusion

So what can be done? Disinformation is not going away, it's cheap, effective, achieves our adversaries' goals. There are things that can be done to if not deter, then to get ahead of these repeated false narratives. but will have to be a whole of society effort from the government, industry, users across our alliance. And there is no silver bullet—rather we must employ multiple layered defenses.

Much like deterring chemical or biological weapon use, when we would never respond in kind to this type of weapon, but rather, we layer defenses of interdiction and attribution, messaging and arms control; that makes an adversary less certain of its success with this weapon. Similarly for countering disinformation, we need to layer our defenses to gain the information advantage. We all have a role in being part of that layered solution.

I'd like to mention four of the solutions that, together, can bolster our defenses: **partnerships, education, technology, and strategic communications.**

1) First, **Partnerships**, we are stronger together. Especially when the fight is occurring in the borderless online world. Russia seeks to undermine partnerships and alliances it sees as against its interest, and it is more important than ever to commit to combatting disinformation together. One great success was in the recent signing of Memorandum of Understanding (MOU) between the United States and Bulgaria that increases cooperation to counter foreign information manipulation.

2) Education—As democracies, we need to make sure our citizens have the tools and ability to utilize social and traditional media and be able to identify good sources of information

Education is a long term, generational challenge. But tools do exist today to educate on media and digital literacy and countering disinformation best practices including graphic novels and computer games, including one that was made by the US State Department called Harmony Square. It is a free, online computer game that teaches how mis and disinformation spreads. It has hundreds of thousands of plays, and it has recently released it in Romanian and Latvian languages, in addition to the available versions in Czech, Dutch, English, French, and German.

These tools build on the idea of inoculation, focusing on the tools to spot manipulated media and make them think twice about sharing manipulated content. Education will be one of the most impactful solutions to make us resilient to disinformation.

3) Technology— Disinformation is going to spread faster and be more complicated when we factor in the role of deep fakes, ChatGPT AI, and whatever comes next. We should invest in technologies that pace with the evolving disinformation threat and working with parts of the government and industry partners who can help us utilize AI and machine learning technologies to more quickly detect narrative patterns and give us more time left of narrative boom to put out our own positive message.

4) Finally, and crucially, Strategic communications
We have to be better at telling our story. Too often NATO's message is communicated in pages of dry, black and white text, and unshareable on social media and that is wholly insufficient in the current digital age. We can find creative ways to share our positive message in ways that resonate and can be easily shared, especially on complicated technical topics like WMD.

We must expect and anticipate that Russia will continue to spread disinformation and sow discord in areas that are full of fear and strong emotion—including WMD topics. And we can use this knowledge to our advantage in crafting strategic messaging that gets ahead of false narratives about nuclear sharing arrangements in NATO, or public health laboratories in NATO countries, or accusations from Russia of arms control violations.

Disinformation is the new normal so we must think about how we can be resilient to this challenge, and by layering multiple defenses we can achieve the information advantage.

As we seek to counter the threat of disinformation, we must keep in mind the goals Russia seeks to accomplish: to divide and weaken the resolve and unity our alliances, and undermine democratic principles. It will be vital, therefore, to ensure all solutions to disinformation protect the values of individual liberty, democracy, human rights and the rule of law.

In our solutions, we must never resort to digital authoritarianism to address this challenge. But we can layer our defenses and better utilize the information

environment, platforms, and understanding of how information spreads to help share our fact-based, positive message in a way that stays true to our values of democracy.