TO: National Security Decision Makers
FROM: Marina Favaro
DATE: January 12, 2022
SUBJECT: Strengthening the OSCE's Role in Strategic Stability

---

Last fall, the Scowcroft Center for Strategy and Security hosted a private workshop with several international experts and officials to discuss how to strengthen the OSCE's role in strategic stability. This paper is designed to give policy makers a better understanding of how emerging technologies should factor into forthcoming arms control regimes.

Strategic Context: The OSCE's Present Role in Strategic Stability

The Organization for Security and Cooperation in Europe (OSCE)—an organization born at the height of the Cold War—might yet again prove instrumental in strengthening strategic stability in the twenty-first century. Shifts in global polarity, a growing role for non-traditional actors, and the unique properties of emerging technologies are all conspiring to undermine strategic stability. Meanwhile, the OSCE's instruments for upholding strategic stability—including common norms, values, and principles of strategic restraint—are eroding in now-defunct treaties. Today, there are a range of material roadblocks to arms control, but the most significant impediment is the current lack of political will to sustain and improve it. At the OSCE, Russian obstructionism is perhaps the clearest manifestation of this trend. The categorical failure of great and middle powers to expend the time, expertise, and political capital necessary to create meaningful regimes of control is stark. It is also, fortunately, something that the OSCE can address and improve. We cannot give up on the OSCE vision of a Europe whole, free, and at peace.

Defining strategic stability

In the Cold War, the stable nuclear deterrence relationship was defined as the ability of the United States and the Soviet Union to survive a first strike and retaliate (i.e., 'survivable second strike'). For Thomas Schelling and others, strategic stability had two components: crisis stability (wherein escalation was unlikely) and arms-race stability (wherein neither side sought a military advantage to either launch a decapitating first strike or to be completely invulnerable to attack). However, emerging technologies, new actors, and the growing complexity of systems are bringing us further from the Cold War context from which this concept emerged. Today, strategic stability is more complex: the concept is no longer defined in solely nuclear terms, but rather incorporates all five operating domains and acknowledges that emerging technologies might increase the vulnerability of nuclear arsenals.

Defining emerging technologies

There is no universal definition for 'emerging technologies,' but this memo defines them as technologies and technological applications that are still under development or are not well-established, and have the potential to disrupt global stability and security. Critically, the range of systems with relevance to strategic stability has broadened as a result of technological change. Whereas traditionally only nuclear weapons constituted a strategic capability, there is a growing awareness that emerging technologies can pose a threat to nuclear forces and related capabilities (e.g., early warning systems, command-and-control systems, and critical infrastructure). This includes new technologies with the potential to disable or intercept a nuclear delivery system and undermine states' ability to survive a first nuclear strike and launch a retaliation.

The intersection of strategic stability and emerging technologies

Emerging technologies are disrupting strategic stability in the following ways:
1. The ability of emerging technologies to reduce the confidence of nuclear powers in their own deterrent or their ability to respond to a nuclear attack. The notion of a 'survivable second strike' is foundational to strategic stability.[1]
2. Their ability to rapidly escalate an ongoing conflict, either deliberately or through miscalculation.[2]
3. Their ability to change the incentives for a given state to increase the quantity or quality of their nuclear forces (i.e., prompt an arms race).[3]
4. Their ability to challenge the moral and legal expectations of appropriate conduct as regards the use of force.

Regulating emerging technologies

Challenges for arms control today

Amid the variance and pace of development in emerging technologies, and the shift to a more confrontational geopolitical landscape, many are understandably concerned with the capacity of arms control to affect positive change. In short, they fear it is too slow, too unresponsive, and too unpopular to adequately address current and future challenges. Some of the specific challenges for arms control of emerging technologies include:

---

[1] See, for example: https://tnsr.org/2021/10/the-standstill-conundrum-the-advent-of-second-strike-vulnerability-and-options-to-address-it/.

[2] See, for example: https://www.kcl.ac.uk/csss/assets/weapons-of-mass-distortion.pdf.

[3] See, for example: https://ifsh.de/en/research/arms-control.

- **Lack of political will.** The central challenge is not lack of dialogue or communication at the OSCE, but a lack of political will. States don't share the same values, principles, or threat perceptions anymore, as evidenced by Russian obstructionism.[4]
- **Quantification and verification.** Some of these innovations (e.g., artificial-intelligence-enabled military technologies) pose a unique challenge to arms control because they are not as easy to quantify or monitor, compared to other weapons systems (e.g., intercontinental ballistic missiles) that are currently limited by arms control agreements. This also makes verification more difficult.[5]
- **Level of analysis.** Capturing a given capability and its risks or opportunities in the language of a treaty is no easy task, and it only gets more difficult as we forecast further into the future (i.e., technology applications and implications become less clear the further away they are). Should we be regulating use cases? Enabling technologies? Behaviors? Whole domains?
- **Pace of technological change.** Humans have been consistently bad at forecasting, especially those futures that do not benefit us. Given the rapid pace of technological change, decision makers might find that after months or years of negotiating an arms control agreement, the outcome is out of pace with the technological reality, particularly for a treaty that is based on technical characteristics. This would render the arms control measure obsolete from the beginning.[6]
- **Pace of negotiation** lags significantly behind the pace of technological change. For example, at the United Nations (UN), negotiators have been debating lethal autonomous weapons systems (LAWS) for nearly a decade and still haven't reached a consensus on what qualifies as LAWS and what use cases are admissible.[7]
- **New actors.** The relentless and accelerating drive to develop new technologies is partially attributable to the actors who are driving innovation. Whereas defense innovation used to primarily flow from public sector to private sector, this direction has been reversed. Private sector actors are motivated by different incentives. If the public sector does not coordinate closely with the private sector to jointly address the potential harms of dual-use technologies, then commercial off-the-shelf (COTS) technologies could become an unwitting part of another state's foreign policy or non-state actors' foreign policy objectives.[8]
- **Private-sector PR and IP concerns.** The private sector develops most of the technology that underpins AI military technology applications. It has also been reluctant to

---

[4] See, for example: https://www.state.gov/on-russias-obstructionism-at-the-organization-for-security-and-cooperation-in-europe/.

[5] Naysan Rafati, "The Arduous Path to Restoring the Iran Nuclear Deal," Arms Control Association, April 2021, https://www.armscontrol.org/taxonomy/term/84?page=2.

[6] Vincent Boulanin, "Regulating military AI will be difficult. Here's a way forward," Bulletin of the Atomic Scientists, March 3, 2021, https://thebulletin.org/2021/03/regulating-military-ai-will-be-difficult-heres-a-way-forward/.

[7] Ibid.

[8] Marina Favaro, "Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction, and the global nuclear order," King's College London, Centre for Science and Security Studies, 2021 Edition, https://www.kcl.ac.uk/csss/assets/weapons-of-mass-distortion.pdf.

participate in regulatory efforts on military AI for a range of reasons, including public relations (PR) and intellectual property (IP). On the former, many companies have shied away from participating in the lethal autonomous weapons debates at the UN out of fear of being branded as 'killer robot' developers.[9] On the latter, IP protects more than just an idea or a concept; it protects valuable business assets that are often central to the services of an organization and its long-term viability.[10]

- **Weight of great powers.** Mounting tensions between militarily advanced giants Russia, China, and the United States make it difficult to imagine these states engaging in a constructive manner on discussions that seeks to manage the risks associated with emerging technologies.
- **Contending with sub-conventional tactics.** There are a range of challenges associated with technologies in the digital information space, which could increase the likelihood of alternative and less predictable escalatory pathways.

Principles for arms control today

- **Disaggregate the impacts of emerging technologies.** In the existing literature, there is a widespread tendency to discuss emerging technologies either "as an abstract, monolithic risk category or via individual cases that supposedly represent the entire category. Neither approach is advancing the conversation on which technologies could impact nuclear strategic stability, and in what ways."[11] Treating emerging technologies as a broad risk category is not particularly helpful because states have limited resources and limited political will to pursue arms control across the entire range of emerging technologies. This underscores the importance of prioritization exercises to disaggregate the impacts of emerging technologies on strategic stability.
- **Give particular attention to hybrid threats.** In the immediate future, the OSCE should continue thinking about the extent to which hybrid threats could have societal and institutional impacts. For example, critical infrastructure vulnerabilities (e.g., water, hospitals, electricity, mobile telecommunications, banking, etc.) can be weaponized to create mass disturbances with both societal and military implications (i.e., could make decision making much more difficult). Furthermore, a combination of disinformation and cyber attacks can produce a dangerous degree of confusion, with negative impacts on military decision making. The disturbances created by these hybrid threats will have a big impact in democratic societies where government decisions are dependent (in part) on public opinion.
- **Situate emerging technologies within a political context.** In determining whether emerging technologies could escalate an ongoing crisis, the key factor is not necessarily the technology itself, but the uncertainty generated by technological innovation and the

---

[9] Boulanin, "Regulating military AI will be difficult."
[10] "Technical Surveillance Counter Measures," Advanced Corporate Solutions, July 2017, https://acsolutions.co.za/news2017/Newsletter-July-2017.pdf.
[11] Favaro, "Weapons of Mass Distortion."

intersection of that uncertainty with the political context. In fact, "emerging technologies are not an independent, primary driver of otherwise avoidable escalation… instead technology functions as an intervening variable—a sometimes necessary, but rarely sufficient, condition for escalation."[12]

- **Avoid pessimism and presentism as regards emerging technologies.** Not all emerging technologies will create risks for strategic stability. In fact, some will create opportunities for augmenting strategic stability. Efforts are necessary to mitigate the risks associated with emerging technologies, while also remaining cognizant of the potential benefits of innovation. Furthermore, those who research and campaign in this field should work to avoid presentism. There is a tendency to view this period as one of unprecedented complexity, but this discourse typically overstates the challenges of today and understates those of the past.

- **Accept different threat perceptions as a basis for bridge-building.** Not all states need to ascribe to the same threat perceptions, but they must believe that all threat perceptions are equally real and legitimate. A classic example of this is Russia's belief that missile defenses in Southeast Europe are aimed toward them, even though the United States continues to affirm that the Aegis system is not focused on Russia. This has tangible ramifications for nuclear stability talks between the two states.

- **Think about arms control at the device and domain levels.** When thinking about arms control from the device level, it is worth asking: How will those in the military or supporting roles know if there is an autonomous capability in the system? Could there be an equivalent of a 'nutritional label' to understand what is in AI-enabled systems? In terms of domain, should we have AI-weapon-free zones? How can we ensure those measures in situations where verification is not possible? These questions are worthy of consideration.

Recommendations for the OSCE

- **Develop CBMs.** Formal treaties are the gold standard of regulation: explicit and enforceable legally binding agreements between state parties to limit the number or potency of a particular weapon. Critically though, we cannot limit our ambition to treaties alone. Even if possible, treaties may take years to negotiate, complicating their ability to control the development trajectory of a rapidly emerging technology. Fortunately, confidence-building measures (CBMs) can be undertaken to precede, bolster, or (partially) substitute treaties. Among international organizations, the OSCE is distinctive in its history for leveraging CBMs for risk reduction. Through CBMs, the OSCE can move the ball forward between like-minded states (e.g., on information operations and emerging technologies) until we see a different type of engagement from Russia on this set of issues. Modernizing the Vienna Document is the obvious place to start.

---

[12] Caitlin Talmadge, "Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today," *Journal of Strategic Studies* 42 no. 6, August 22, 2019, https://www.tandfonline.com/doi/abs/10.1080/01402390.2019.1631811.

- For example, the OSCE could focus on **CBMs for autonomous weapon systems**. The Vienna Document could expand its scope to include information and communications technologies. This could involve a voluntary exchange of information regarding the nature of autonomous systems (e.g., target, decision to engage), human ability to override (i.e., on the loop vs. in the loop), and greater transparency on elements of command and control to avoid inadvertent escalation.
  - Furthermore, to mitigate the risks of crisis escalation, relevant states should develop additional **crisis communication channels** focused on the ability of emerging technologies to rapidly escalate an ongoing crisis.
  - Finally, it is important to note that confidence-building and arms control are not replacements for deterrence; they need to work together.
- **Bridge the divide between policy folk and technical folk.** Many emerging technologies originate in an ecosystem that is fundamentally different from the traditional defense industrial model, which was more top-down in nature, with a small number of sellers and a single buyer, typically the military. In contrast, many emerging technologies are already being developed in the private sector, often by multinational companies that have not traditionally worked for defense. This is a more bottom-up model.[13] The public sector in OSCE member states must therefore be able to communicate with the private sector about the potential harms of dual-use technologies and explain why it may be worthwhile for a wider range of defense suppliers to consider the security needs of society. On the supply side, this could involve changes to national educational curricula to include technology ethics and human-centred design. On the demand side, there need to be more, and better-paid, roles for scientists and technologists who want to work in public policy, in government agencies, and legislative staffs.[14] The policymakers responsible for negotiating CBMs on these issues need to have a better understanding of the opportunities and limitations presented by new technologies.
- **Use foresight methods to explore possible futures.** Given the uncertainty surrounding the future strategic environment, it is more important than ever that scholars and practitioners have the tools to anticipate what the future might hold. 'Foresight' refers to insights into how and why the future could be different from today. This, in turn, helps to improve policy, planning, and decision making. Critically, foresight methods such as wargaming and scenario planning enable us to look beyond our own perspective to consider the interests, threat perceptions, and strategic approaches of other stakeholders. This is highly relevant to the OSCE, where gaming could help states to identify how, for example, Russia might react in a given scenario. Relatedly, discussions about strategic stability could be brought alive through fiction, which enables us to expand our imagination and explore possible futures without invoking suspicion in our adversaries. Such approaches could disrupt more conventional views of security and shake up static

---

[13] Favaro, "Weapons of Mass Distortion."
[14] Ibid.

thinking, while working toward meaningful participation from a diverse group of stakeholders, to forecast a holistic future.[15]

Conclusion

States are likely to see technological developments as undermining their security and to resist arms control efforts. Instead, they will prefer to play catch-up or develop their own technological capabilities and advantages. As such, the prospects for arms control in the short term are bleak. But as political circumstances evolve and the costs of an arms race increase, arms control becomes increasingly attractive. The OSCE is uniquely placed to advance certain measures that could help manage the challenges to stability caused by emerging technologies.

Marina Favaro is a nonresident fellow with the Transatlantic Security Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security and a research fellow at the Institute for Peace Research and Security Policy at the University of Hamburg, where her research focuses on the impact of emerging technologies on arms control.

---

[15] Marina Favaro and Sara Z. Kutchesfahani, "We can't prevent tomorrow's nuclear wars unless we imagine them today," Bulletin of the Atomic Scientists, August 26, 2021, https://thebulletin.org/2021/08/we-cant-prevent-tomorrows-nuclear-wars-unless-we-imagine-them-today/.