

Testimony for CSCE Field Hearing on “AI, UAVs, Hypersonics and Autonomous Systems:
Emerging Technologies and Euro-Atlantic Security”

Arlington, Texas

January 22, 2020

By

William Inboden, Ph.D.

*Executive Director at the Clements Center for National Security and Associate Professor at the
LBJ School, University of Texas-Austin*

I.

Congressman Veasey, other Commissioners, and invited guests, thank you for including me in today’s hearing on this most important of topics.

On April 27, 2007, Estonian citizens found themselves and their country under attack. External threats were all too familiar to this tiny Baltic State, which had been invaded and occupied for most of the twentieth century by Nazi Germany and the Soviet Union. But this attack was different. It was not tanks and troops rolling across the border, or airplanes dropping bombs from the sky, but computer signals travelling at the speed of light through internet cables. In short order, the cyberattacks disrupted or shut down entirely Estonia’s banking system, government, major media outlets, and political parties. These attacks continued in waves for three weeks. Though not a bomb was dropped or shot was fired nor did a single enemy soldier set foot in the country, the effects were crippling and brought the country to a standstill. For Estonia the effect was almost the same of being invaded, occupied, and controlled by an outside power.

That outside power was Russia.

Vladimir Putin, with his endless pile of grievances, saw Estonia as a quadruple violator. He objected to Estonia joining NATO three years earlier, resented Estonia’s independence from the former Soviet Union in 1991 (when Estonia also became an OSCE participant), and still seethed over what he saw as Estonia’s betrayal of his father during the elder Putin’s military service in the Estonian territory during World War II. And most recently, in the proximate cause of the cyberattacks, Putin took umbrage at Estonia for moving a statue of a Red Army soldier from the center of Tallin to the outskirts. Putin saw the statue as a tribute to Russian valor in World War II; Estonians saw it as an ugly reminder of the Soviet Union’s occupation and tyranny over their country.

Though thirteen years after the onslaught on Estonia many operational details are still unknown (that in itself being one of the hallmarks of cyber warfare), what is not disputed is that the Kremlin was the originating, authorizing, and orchestrating power behind the attacks. As the

historian Robert Service writes, “the Kremlin’s purpose was not only to knock out the Estonian network of communications but also to show the world what it could do – as well as to allow its disruptive specialists to conduct a real-life test of what became known as hybrid warfare. *Without setting foot outside the Russian capital they could do enormous harm abroad.*”¹

History, it has been said, is lived forward and understood backwards. In that spirit, and for purposes of this hearing, from our vantage point of thirteen years later we should look back on Russia’s cyberattack on Estonia and see it for what it was: the first wave in what would become a cascade of Russia aggression and hybrid warfare that included weaponizing new technologies. The Estonia attacks were followed by, inter alia, Russia’s invasion of Georgia in 2008, intervention in Syria in 2013, seizure of Crimea and assault on Ukraine in 2014. Perhaps we might add to this list Russia’s assault on our democratic processes in the 2016 election, an assault that continues today. Though the particulars of each act of aggression varied, each included the use of new technologies and escalating levels of sophistication, all for the purposes of projecting Russian power, securing Russian interests, and weakening Russia’s (perceived) adversaries.

Thus what began with the use of cyberwarfare against Estonia, became cyberattacks followed by land invasion and precision weapon employment in Georgia in 2008, and then with increasing sophistication the use of autonomous weapons and UAVs in the invasion of Ukraine in 2014 and the intervention in Syria in 2015.

I begin with these observations because, though Russia is not mentioned by name in the title of today’s hearing, Russia is the OSCE state most implicated in the themes and questions we are addressing today. Russia is the OSCE state most involved in researching and developing these new weapons systems, most involved in employing them, and arguably most resistant to current or new measures or agreements to control and limit their use. It also bears noting that, with the exception of Syria, all of the states toward which Russia engaged in this aggression are also OSCE participants.

The other OSCE participant state leading in the development of these technologies is the United States.

II.

Why does this matter? I am not an expert on technology or defense policy; my training, experience, and research focus sit at the intersection of history, strategy, and statecraft. The focus of my testimony is on the strategic and diplomatic implications of these emerging technologies.

History reminds us that technological innovation in weaponry is a near constant factor in warfare and statecraft. Past innovations such as the long bow, the crossbow, gunpowder, repeating arms, tanks, submarines, aircraft, jet propulsion, ballistic missiles, nuclear age, all brought various revolutions in warfare and force projection. If anything, innovation in weaponry

¹ Emphasis added. Robert Service, *Kremlin Winter: Russia and the Second Coming of Vladimir Putin* (London: Picador 2019), 263-264.

is a constant factor in history, as is the human propensity for violence. The details will change, but these questions will always bedevil us in some form or another.

Anytime we make a strategic assessment of emerging technologies, we should ask ourselves: What is new, and what is not?

I begin with that which is not new:

- **Lethality:** These emerging technologies do not have unprecedented levels of lethality. As grim as it is to contemplate, the “lethality threshold” was crossed decades ago with the development of chemical, biological, and thermonuclear weapons, all of which can cause mass casualties on a terrifying scale.
- **Range:** These emerging technologies do not have unprecedented levels of range and reach. Existing weapons systems already enable the projection of force globally, and for over a half century we have had reach into outer space as well.
- **Speed:** Though emerging technologies under consideration involve varying dimensions of speed, whether in information processing or projectile velocity, they do not represent a qualitative leap in rapidity. Ballistic missiles already fly at several times the speed of sound. The internet already offers communications at the speed of light. Though some aspects of these new weapons have elements of rapidity – such as the blend of speed, mobility, and precision guidance of hypersonics, the speed by itself is not new.

So what is new? I believe the following factors are distinctive and to a degree unprecedented; they are not exhaustive but rather illustrative of the new strategic dimensions wrought by these emerging technologies:

- **Deniability.** Given various factors including the distance of human operators, the operational complexity that can involve cut-outs and false surrogates, and the literal autonomy of some of these systems, many of them offer a new dimension of deniability and potential anonymity that previous generations of weapons systems did not. This in turn makes deterrence and retaliation more difficult, and can be strategically destabilizing.
- **Controllability.** This is a corollary of deniability; these new weapons systems can be controlled remotely with greater precision, from greater distance, with greater anonymity, and in greater safety for the operators, than any previous weapons by an order of magnitude. It means that kinetic action could be taking place in an OSCE participant state but controlled by various actors 10,000 miles away in multiple directions.
- **Inhumanity.** This is meant not in a melodramatic manner but in the very literal sense of removing the human actor in ways never before seen. The closest past parallel came when the Soviet Union experimented in the 1980s with the infamous “Dead Hand” of its Doomsday machine that would have put the Soviet nuclear arsenal under automated control to launch automatic retaliatory strikes even if the entire command and control system had been decapitated. But while UAVs at least for now have human controllers, the emerging domain of AI and autonomous weapons brings in a new paradigm that may completely

remove the human actor and thus be quite literally “inhumane.” Paul Scharre of the Center for New American Security puts it this way: “do we control our creations or do they control us?”²

III.

How, then, should the OSCE think about these emerging technologies?

I will state my central point up front: the importance of these emerging technologies cannot be evaluated aside from the nature of the states that use them.

It is not the fact of the new technologies that matters most, but who will use them and for what purposes. It is not the nature of these weapons that should primarily concern us. It is the nature of the regime that possesses and deploys them.

To put it more pointedly and perhaps provocatively, I doubt that many if any of us here today lose sleep over the fact that the United Kingdom and France (both OSCE participant states of course) possess nuclear weapons. Whereas many of us do continue to worry, with warrant, about Russia’s nuclear arsenal (and likewise the DPRK’s nuclear arsenal, though they are not an OSCE participant).

This, of course, was the core strategic insight of the original Helsinki process, connecting as it did respect for human rights and civil liberties with European and transatlantic security. It also continues to be the animating spirit of the OSCE.

For this reason Putin and Russia occupy a large part of my testimony. Of the OSCE participating states, Russia and the United States are by far the most active and advanced in researching, developing, and deploying these emerging technologies. All OSCE participant states must participate in addressing these trends, but the conversation and consideration should focus on where these new weapons are most prevalent and most frequently employed.

To understand why Russia has been and continues to be so active in this realm, one must start with Vladimir Putin and how he sees the world. As many Russia scholars and Putin biographers have observed, the Cold War exerted – and continues to exert – a profound influence on the Russian leader. It provided his formative professional experiences as a KGB officer, and now provides a ready set of historical insights, lessons, and grievances for his worldview and statecraft.

One of the Cold War lessons Putin obsesses over concerns how the American technological edge proved decisive in the arms race that contributed to the Soviet Union’s bankruptcy. It was not just that by the 1980s the US began outspending the Soviets in dollars to rubles for the military; it was that the US developed a qualitative edge in defense technology that meant no matter how much the Soviets spent, they could not keep pace with the new advances in American weapons systems – from stealth, to precision guidance, to submarine quieting, to the lofty ambitions of the Strategic Defense Initiative. This was in part why the Kremlin resorted to

² Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton 2018), 8.

stealing Western technology through a massive KGB espionage campaign. Even these purloined technologies, however, bumped up against the constraints of the Soviet system and its sclerotic economy. As Fiona Hill and Clifford Gaddy document in their biography of Putin, he and his KGB colleagues became frustrated “that the Soviet economic system was incapable of using the technology stolen from the West.” Putin is determined now not to let Russia fall into that same trap.³

In particular he does not want to see the traditional Western technology edge once again overmatch Russia as in the Cold War. Putin seeks to make technological advancement central to the Russian military-industrial complex, central to Russian military strategy and doctrine, and central to Russian power projection.

Cost matters too. As sophisticated as they are in technological terms, these new weapons are relatively cheap compared to the cost of training equipping maintaining large conventional forces. This appeals to Putin given Russia’s economic stagnation and limited financial resources, in light of its imbalanced economy and ongoing pressure from Western sanctions.

Additionally, Russian military doctrine and Putin’s strategic designs depend in part on integrating the use of these new technologies for employment in “grey zone” conflicts and hybrid warfare. UAVs can be used for everything from kinetic operations that kill adversaries, to monitoring contested spaces for information operations and political warfare. As Jeff Edmonds and Samuel Bendett of the Center for Naval Analyses have written, “with greater access to space-based information, unmanned aerial vehicles, airborne reconnaissance systems, command and control systems, and unparalleled developments in electronic warfare, the Russian military is equipped to detect, track, and influence developments across the battlefield.”⁴ Russia is using its interventions in Ukraine and Syria as battlefield laboratories for testing and refining these emerging weapons technologies.

Finally, Putin’s authoritarian rule squelches and silences any dissent, and empowers him to act with aggression based only on his whims, preferences, or designs. Because he lacks popular legitimacy – and because he fears his own citizens – he resorts to a perverse and toxic combination of cultivating grievances, fueling paranoia, and projecting strength against adversaries real or perceived. Such a ruler naturally seeks to acquire – and potentially to use – the most advanced, sophisticated, and lethal weapons systems that he can.

IV.

The best framework to address these emerging technologies lies in the commitments and values embodied by the Helsinki Final Act. Open, free, and secure societies are best equipped to explore, debate, wrestle with, and ultimately resolve these hard questions.

³ Fiona Hill and Clifford Gaddy, *Mr. Putin: Operative in the Kremlin* (Washington DC: Brookings Institution Press 2015), 143.

⁴ <https://thestrategybridge.org/the-bridge/2019/2/26/russian-battlefield-awareness-and-information-dominance-improved-capabilities-and-future-challenges>

In particular, Principle VII's guarantee of freedom of thought, conscience, religion, or belief protects the rights and capabilities of religious believers, alone or in fellowship, to draw on transcendent insights and act as prophetic voices of conscience for their societies. They can apply moral and religious principles to the just use of force, restraint on the use of force, and how human dignity can be either protected or exploited by emerging weapons technologies. It similarly empowers other dissenting voices, religious or secular, to raise hard questions, interrogate received dogmas, and engage in the creative thinking necessary to ensure that these new technologies – with their awesome power to create and to destroy – serve and secure free societies.

Principle VII's affirmation of "the effective exercise of civil, political, economic, social, cultural and other rights and freedoms, all of which derive from the inherent dignity of the human person and are essential for his free and full development" creates further space for open societies to address the challenges presented by emerging weapons technologies. Placing the human person – rather than the state, the ruler, the technology, or any other such alternatives – at the center of the Helsinki process provides a foundation for exploring how best to manage these new weapons systems. It answers the hard question posed by Scharre, and affirms that we need to control our creations.

In contrast, authoritarian states by their nature brook little dissent, encourage little transparency and debate, and concentrate power in the hands of dictators or ruling cliques that generally make decisions on the development and employment of arms based on expediency and utility more than morality or conscience.

In practical terms, any strategy to address Russia's growing advantage in this weaponry needs to include pressing Russia to honor its OSCE commitments on human rights and freedoms.

V.

Finally, how might these technologies be managed and perhaps limited by international agreements?

This question is even more complex than many other arms control questions because many of these emerging technologies have important civilian applications. In the private sector the technology itself will continue to be developed, refined, and used. In many cases in these civilian contexts it will contribute to economic growth, prosperity, and human flourishing. The question is whether the weaponization, the lethal use of it by militaries, can (or even should) be controlled?

On this question, I conclude with a hope, a caution, and a recommendation

- A hope: International agreements are possible. They have been forged at times in the past on controlling new weapons technologies. Whether sawtooth bayonets, dum-dum bullets, chemical and biological weapons, blinding lasers, or even the entire class of nuclear weapons abolished by the 1987 INF treaty, competing states have been able to come together, forge agreements, and honor and fulfill them.

- A caution: An arms control agreement is only as strong as its weakest signatory, and its verification regime. While Russia would need to be part of any effective arms control accords on emerging weapons technologies, Russia also historically has a bad habit of treaty violations. These include its violations (either in its previous incarnation as the Soviet Union or now as Russia) of the ABM treaty, the Biological Weapons Convention, and the INF treaty, not to mention its serial violations of its OSCE commitments. We should temper our expectations and hopes of just how much can be accomplished with Russia in this realm.
- A recommendation: The United States and like-minded OSCE participant states should take a page from the Cold War playbook and combine strength with diplomacy. Diplomatic success proceeds from military power and allied unity. To begin, the United States and other OSCE democracies should move forward in developing our own capabilities on emerging weapons technologies, specifically those featured today: AI, UAVs, Hypersonics, and Autonomous Systems. Unilateral disarmament is not a luxury we can indulge. But, as with the NATO “dual track” decision of 1979 to respond to the Soviet deployment of Intermediate Range Nuclear Missiles in Europe by deploying US Pershing IIs and Ground Launched Cruise Missiles and also pursuing diplomatic negotiations with the Soviets, today we are in a similar strategic predicament. We need to build-up to negotiate. From a position of strength we can better encourage Russia and other potentially recalcitrant states of the advantages of setting shared rules for the control, use, and limitation of these weapons.

Thank you for your time and interest, and I look forward to your comments and questions, and our discussion.