National Security in the Modern Age: An Interview with Dr. Joshua Geltzer, Former Legal Advisor to the National Security Council

Interview by Colby O'Connor

Biography

Dr. Joshua Geltzer is a partner at the law firm WilmerHale, where his practice centers on national security as well as artificial intelligence and other emerging technologies. Prior to joining WilmerHale, Dr. Geltzer served in senior roles at the White House, including as Deputy Assistant to the President, Deputy White House Counsel, and Legal Advisor to the National Security Council (NSC) under the Biden administration as well as Deputy Homeland Security Advisor. Dr. Geltzer also served as Senior Director for Counterterrorism and Deputy Legal Advisor to the NSC under the Obama administration. At the White House, he advised on subjects such as counterterrorism, hostage negotiation, critical infrastructure protection, and the intersection of advanced technologies and national security.

In addition to his work in government service, Dr. Geltzer was the founding Executive Director of Georgetown Law's Institute for Constitutional Advocacy and Protection, where he served as a visiting professor of law. Dr. Geltzer holds a bachelor's degree from Princeton University, master's and doctorate degrees in international relations and war studies from King's College London, and a J.D. from Yale Law School.

1. *To begin, can you describe how you first began working with the National Security Council?*

Sure. My first chance to go over to the National Security Council was in 2015, a decade ago now, when I joined the legal team there. The legal team traditionally consisted mostly of national security lawyers "on loan" to the White House from different parts of the executive branch: from the Defense Department, the State Department, the intelligence community, and, in my case, the Justice Department. Having spent some time in the National

Security Division at the Justice Department, including working with the National Security Council's legal team and others, I got a chance to work with the NSC legal team starting in early 2015.

2. *Given the high pressure and impactful nature of your work under the Biden administration, is there a specific decision or moment from your time in government that you find most memorable or defining?*

There are a few, some are very specific, and some are at a much broader or more strategic level. Specific moments that I think were very gratifying for a lot of us involved were when Americans held hostage or wrongfully detained abroad came home. It's an issue for which I have particular passion, as did many others in the Biden administration. When you're working on those cases, you have a lot of very tough days, but if you stick with it, and you have a president willing to make hard choices the way President Biden was—that enables Americans to come home—then you get a really good day where those individuals emerge from really unimaginably hard circumstances, returning to U.S. soil and to their loved ones. That is very fulfilling and gratifying to see. There were also days that were meaningful in other ways. For those of us who've been part of the counterterrorism mission in various respects, seeing overdue justice done with respect to Ayman al-Zawahiri [for example,] represented an important moment for a lot of us who've been part of counterterrorism issues.[1]

Then there are things at the more strategic level. When one issue is part of building an executive order or a national security memorandum, that is satisfying in its own way. In particular for me, working on the National Security Memorandum on artificial intelligence was a really fascinating and meaningful project, and seeing it issued by President Biden was quite rewarding.[2]

---

[1] Ayman al-Zawahiri was killed by a U.S. launched drone missile strike on July 31st, 2022 in Kabul, Afghanistan. He was the second in command at Al-Queda at the time of the 9/11 attacks, and became the leader after the death of Osama Bin Laden

[2] The memorandum was issued in late 2024, and focused on three main policy objectives. It sought to maintain U.S. AI leadership, accelerate AI use across National Security Agencies, and develop AI safety and governance frameworks to support national security. The document also focused on how and when AI could be used by national security agencies in order to establish a balance between security and privacy. See "DCPD-202400945 - National Security Memorandum on Advancing the United States," Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence," *Office of the Federal Register, National Archives and Records Administration*, October 23, 2024. https://www.govinfo.gov/app/details/DCPD-202400945.

3. *You mentioned your involvement in negotiations to release American hostages during the Israel-Hamas conflict following the October 7 attacks. Could you further describe that experience of managing such a high-stakes and instrumental moment?*

There was so much to deal with as a government in the immediate wake—and frankly, for weeks and months to come—after October 7. Among [the administration's] priorities, a really high priority was getting out the Americans who were held by Hamas. The Biden administration felt that, while our goal, of course, was to get all of them out as quickly as we could, there was a near term opportunity to get at least some out particularly swiftly. That's what you saw us able to do. We worked with partners in the region, who are often the key to negotiating, sometimes indirectly, with bad actors in the world like Hamas. We were able to get some Americans out quite swiftly, even if it took literal years, unfortunately, to get other hostages out. I do think it's a testament to the commitment of the U.S. government that—even when dealing with something as big-picture and with as massive a set of regional and strategic ramifications as the October 7 attacks had—we simultaneously dealt with the really granular: the particular Americans who were in unspeakable conditions being held by Hamas. [We also dealt] with their loved ones, who were understandably beside themselves and wanted to make sure that we were treating this as an absolute priority and doing so with a sense of urgency, which we also believed we should be doing.

4. *Through your testimony before Congress and your work in the Biden administration, you talked about the transnational terrorist threat of white supremacist networks, and you've likened their methods to those of ISIS and other similar groups. How do you characterize these similarities, and what implications do you think they have for how we think about and respond to terrorism today?*

I start with a fundamental principle that whatever ideology or political view inspires someone, what that person cannot do, no matter their frustrations, is turn violent with those beliefs. That is to my mind, and I think the minds of many of us who work on counterterrorism, the defining feature of [terrorism]. It turns ideological or political views into the one thing that those cannot become in the context of a democracy, which is violence or credible threats of violence. The ideology or political views that inspire people to violence has waxed, waned, and shifted in the United States and in other countries over time. One thing that we started to do, truly on day one of the Biden administration, was to make sure that we were treating all forms of political violence with the urgency they demand, given the threat to public

safety, and democratic integrity they represent. That doesn't mean that you bring all the same tools to [different] manifestations of that problem. It's very different to deal with a terrorist group that's holding territory, having seized it abroad, versus to deal with a network of individuals who want to pursue violence on U.S. soil. In the first instance, the U.S. military might have a very reasonable role to play. In the second, it has none. Intelligence community authorities are going to differ dramatically when one is talking about actions abroad versus threats at home, but starting with the premise that all forms of ideologically motivated or politically motivated violence are unacceptable, we can then calibrate which tools to bring to bear for which threats. That's part of dealing with the hard, multifarious nature of political and ideological violence these days. I do think we see actors across different ideological motivations learning tactics and techniques from each other. In this world of global connectivity, it's very easy [for these groups] to watch each other and even incorporate and adapt some of those same tactics.

5. *You've also written about the role of Russian disinformation in strengthening these online white supremacist networks. What lessons do you think can be drawn from the Biden administration's efforts to address that?*

I do think that foreign governments and foreign actors' efforts to distort and disrupt U.S. democracy—and perhaps even more egregiously, to stoke the embers of violence and threats to public safety at home—should be kind of a unifying rallying cry, whatever one's own views domestically may be. No one should interfere with our democracy, and no one should add to the already substantial problem of those who might turn violent with their ideological or political views, whatever those might be. I do think there are U.S. adversaries and rivals in the world who see an opportunity in harnessing modern technologies to reach into our democracy and pit us against each other, even doing so to the point of trying to exacerbate existing calls to violence. My hope is that over time, our government increasingly disrupts that activity, but also that we as a society are increasingly hardened to those sorts of influence efforts. Ultimately, I do think foreign actors will continue to try to exploit that vulnerability where they can.

6. *So what do you believe that people or the government should do to "become increasingly hardened," against these threats, as you put it?*

At a societal level, I do think there's potential for increased digital literacy and fluency that's going to be necessary as all of us continue to live in an

increasingly digital world. This isn't just a world of national security. This is a world in which there are scams and frauds perpetrated online to dizzying effect, in terms of the dollars reaped in by bad actors, criminal activity, and exploitation of youth. Especially as there's generational change, and a populace that obviously makes use of the extraordinary things available through the internet, people need to be increasingly able to discern fact from fiction, to discern those who might imitate certain actors from the real actors. I think we are going to need that as we live in an increasingly digital world, and we're going to need that as bad actors see those digital tools as points of entry and opportunities for exploitation.

7. *In your view, does combating AI-generated misinformation require a substantially different approach than traditional misinformation?*

I think as a starting point, AI holds both tremendous opportunity and considerable risk. As your question indicates, on the "risk" side of the spectrum is the ability to take disinformation and deep fakes and enhance both their speed and ease of production, as well as their efficacy. What can be done with AI already is quite remarkable. Of course, like most technologies, it will only get better from here. The capacity to have seemingly influential voices weighing in on hot-button issues or even galvanizing people to violence or leading them to doubt the results of an election, could hold real peril. You are rightly asking whether that is different in degree or different in kind from the existing problems of misinformation and disinformation circulating. I do think it ratchets up the challenge here, because we have seen it easy enough in the age of the internet to spread terrorist recruitment materials, for example.[3] It takes this idea of micro-targeting that we see online and ups the ante for it even further—to have AI produce many variations of a terrorist recruitment video or some deep-fake of a celebrity or a politician saying the opposite of what they really believe. I do think that innovation takes an existing problem set and accelerates the challenge posed by it.

8. *You currently work at WilmerHale with a focus on AI and cybersecurity law. How do you think international law can adapt to*

[3] Terrorist groups such as the Islamic State have used social media platforms to spread their ideology through multiple messages, leading to a diversified viewer base that IS can recruit and radicalize at little cost. Michael Steinbach, "ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media," Testimony before the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, Washington, D.C., July 6, 2016, Federal Bureau of Investigation, https://www.fbi.gov/news/speeches-and-testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-.

effectively respond to hybrid effects, including cyberattacks, disinformation, and other emerging tactics?

I'm fascinated by this, and had the chance recently to visit a law school and participate in the symposium on the future of the law of armed conflict, a form of international law. I think AI is injecting some really interesting questions at a really high pace for international law. There's a lot of discussion in the literature already about so-called autonomous weapons systems, and part of what I've seen as a practitioner is that autonomy isn't some event waiting to happen at a particular date in the future. Instead, we've actually had certain weapons systems for years—think of the Aegis missile system and the Patriot system that have degrees of autonomy—that are pre-programmed to respond automatically to certain stimuli for the very reason that the humans would be too slow in the circumstances imagined. So autonomy seems to me a spectrum, not a dichotomy, and it's a spectrum that we are moving along given what AI can do. Again, grounding this as from a practitioner's perspective, rather than debate autonomous weapons systems, yay or nay as a category, I think there's a real burden on lawyers associated with militaries to think about the individual systems that are already being developed and deployed. They have elements in which autonomy appears to get ceded from humans to machines, and lawyers are being asked to rapidly respond and figure out whether we're comfortable with that, and whether those systems are able to meet international laws' demands for things like proportionality, distinction and humanity.[4] I am open to the possibility that some systems, in some circumstances, can meet these standards. They're not categorically incapable of meeting those thresholds, but it requires, to my mind, a much more granular view of particular systems: how they've been tested, how they seem to perform, and what circumstances they would be deployed in. It's a much more granular and contextual question.

9. *Chinese AI policy is more focused on inclusivity and multilateralism, with the global south as well as AI as the driving force for social and economic development and sustainability. Do you believe American AI policy falls short in these areas? If so, what can be done to fix that?*

[4] Humanitarian International law has much of its basis on these three principles. It dictates proportionality, the idea that an action should be responded to with a like action. It also requires distinction between combatants and civilians in times of war, and humanity, the idea that the rules apply even when those affected are not under a specific treaty, as denoted in the Martens Clause. See "Martens Clause," ICRC Online Casebook, Accessed February 17, 2026, https://casebook.icrc.org/a_to_z/glossary/martens-clause.

I might start by contesting the premise a little bit, if you will indulge me. I do think the Chinese engaged in a clever act of public diplomacy releasing a document purportedly focused on multilateral governance and dimensions of AI globally at the same time as the U.S. government released its AI action plan in July of 2025.[5] But I would say two things about what the Chinese released; one, on its own, by its own terms, it was not an "apples-to-apples" document.[6] In other words, this was not claiming to be their version of an action plan. It was instead a release of a document purportedly imagining how there could be greater global governance in AI, whereas the document released by Washington did not purport to be that. It was a document on how to drive AI growth in the private sector and with some role for the government here in the U.S. The Chinese certainly have their own version of that document, it just wasn't what they released that day. The second point I'd make is that I haven't seen a lot of effort put in by the Chinese to actually make real anything in that document. It strikes me more as an act of public diplomacy to counter an AI Action Plan released by Washington, to focus on their alleged commitment to global governance. But here we are, months later, and I don't see a lot of diplomatic "oomph" being put by the Chinese behind global governance. That said, the Chinese and Americans are clearly focusing on AI as a thing of the future, in both private sector and government, a difference which is less distinguishable on the Chinese side than it is on the U.S. side. By a "thing of the future," I mean in economic terms, in national security terms, something where they each want to have the lead. There's probably a good reason for that, given what this technology represents in terms of economic opportunities, economic efficiency, and for national security and public safety. I think that the two governments are probably thinking about it a lot more similarly than those two documents that got released the same day might lead a reader to infer.

[5] The U.S. government released an action plan for artificial intelligence centered around three pillars: innovation, infrastructure, and international diplomacy and security. The plan pushed for deregulation, investment in AI and datacenters, as well as using it to protect U.S. jobs and capabilities. At the same time, it seeks to ensure the U.S. will remain at the forefront of AI technology, through exporting technology to its partners while keeping the technology and semiconductors away from U.S. rivals. See White House, "America's AI Action Plan" (2025).

[6] The Chinese government released a document titled "Global AI Governance Action Plan," which highlighted the need for collaboration between governments, companies, and academia, as well as the need to address energy and environmental issues. It also discussed promoting common norms, and removing bias from AI models. See Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Action Plan" (2025).

10. *Finally, to many students reading Hemispheres, your career trajectory is inspirational. What advice would you give to those who aspire to work at the intersection of law, security and policy?*

Two things, one is to find good mentors and to be a good mentor when the opportunities arise. I have been very grateful in school, in work, but really just in life, to have professors, bosses, colleagues, people who have invested in me, who've given me opportunities when there were surely others interested in those opportunities. They've helped me succeed in those opportunities and have kept offering support, guidance, and insight at critical junctures. I have felt it a responsibility, but also a pleasure, to try to do the same for others, when the opportunities to do so arise. I would encourage readers both to be open to being mentored and being mentors, both of which are lifelong things to do. I think the second thing I'd emphasize is, especially if one is interested in national security, especially if one is interested in the law, and maybe doubly especially if one is interested in national security law, to keep an eye on technology. I do not claim to be a computer scientist, I do not claim to be an engineer. I am not those things, but I have tried to work on and learn about issues at the intersection of technology and national security and the law, because those seem to me to be very, very interesting and consequential, and to be ones where understanding a bit about the technology itself really helps lawyers, who are then relied upon to apply existing law, as written, to those new technologies.

Bibliography

Allen, Gregory C., and Isaac Goldston. "The Biden Administration's National Security Memorandum on AI Explained." *Center for Strategic and International Studies*, October 25, 2024. https://www.csis.org/analysis/biden-administrations-national-security-memorandum-ai-explained.

"DCPD-202400945 - National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence." *Office of the Federal Register, National Archives and Records Administration*, October 23, 2024. https://www.govinfo.gov/app/details/DCPD-202400945.

"Fundamental Principles of IHL." ICRC Online Casebook. Accessed February 17, 2026. https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl.

"Martens Clause." ICRC Online Casebook. Accessed February 17, 2026. https://casebook.icrc.org/a_to_z/glossary/martens-clause.

Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Action Plan" (2025).

Steinbach, Michael. "ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media." Testimony before the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, Washington, D.C. July 6, 2016. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches-and-testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-.

White House, "America's AI Action Plan" (2025).