

A View from the CT Foxhole: Adam Hadley, Executive Director, Tech Against Terrorism

By Don Rassler

Adam Hadley CBE is the Founder and Executive Director of Tech Against Terrorism, a public-private partnership dedicated to disrupting terrorists online. Tech Against Terrorism was established as an initiative of the United Nations Counter-Terrorism Committee Executive Directorate (CTED). Hadley is also the CEO of QuantSpark, an AI innovation consultancy.

CTC: You founded and serve as the Executive Director of Tech Against Terrorism and as the founder and CEO of QuantSpark, a consultancy focused on driving innovation through applied analytics and AI. What led you to the field of terrorism studies and the counterterrorism area?

Hadley: My role in establishing Tech Against Terrorism was entirely unexpected and was born out of work that I was doing, studying in a master's program at King's College London. My background is rather eclectic, having studied physics, Middle Eastern studies, Arabic language, and I worked in a range of public and private sector roles over the years in a number of start-ups and consultancies. But I was studying for a master's in Middle Eastern Studies and found myself focused particularly on analyzing Dabiq magazine. Part of my academic background had been in physics and computer science. So, it's trivial to do some natural language processing, and the idea behind my work at King's was to try to understand the nature of how Islamic scripture had been instrumentalized by jihadists and the topic of abrogation within Islamic jurisprudence and in particular how different parts of the Qur'an and Hadith are used selectively or idiosyncratically by political Islam, and in particular violent Islamism. So, my initial work was focused on this crossover between computer science and Islamic theology and terrorism studies. I think this speaks to what I find interesting and innovative, which is cross-disciplinary work. Much of my professional background has been this mix of social sciences and the physical sciences. This is borne out by a lot of what I've done subsequently.

My dissertation was spotted by an official working at the U.N. Security Council. This was at the heyday of the use of the internet by the so-called Islamic State, of course, and the United Nations Counter-Terrorism Committee, which exists underneath the Security Council, had just started a project looking at how the internet was being used by terrorists. Bear in mind, this is 2016. The sheer volume of terrorist content online was really out of control. So, it's serendipitous in the sense that I was working on a simple computational approach to understand and detect Islamic State propaganda, and I was asked to join a research project working with the U.N., which at the time was just a very small initiative funded by the government of Switzerland.

One thing led to another, and eventually, I grew this project into Tech Against Terrorism. Around the same time, I was also

working as a freelance data scientist—working on applying data science, analytics, and some basic artificial intelligence techniques to solve various commercial problems within a few private sector businesses in London. It was a very busy year, the result of which ended with me founding Tech Against Terrorism and bootstrapping QuantSpark.^a Tech Against Terrorism was accidental in a sense, but I suppose, looking back, its establishment was sort of inevitable given the environment at the time and the need to bridge the gap between government and tech platforms and bridge effectively the intelligence gap with regards to understanding how terrorists were using the internet and what we should do about it.

CTC: Can you talk about Tech Against Terrorism—its mission, where it's been, key accomplishments, and what's next for it?

Hadley: For me, Tech Against Terrorism, whilst its establishment—or at least the initial genesis of the work—was unexpected, environmentally, it was almost inevitable that someone would create this type of organization because there's *such* a gap. There are a number of gaps, really. One is how to work alongside government and tech platforms in a non-combative, collaborative fashion, how to bridge that divide. The other is how to bridge this policy and tech divide, which exists within government, within platforms as well. 'Is there a way of using tech within the social sciences or humanities?' With Tech Against Terrorism, that's what I've been trying to do—trying to create a new type of organization that isn't a not-for-profit, isn't a start-up, but is a combination of these two things that's mission-driven, that's purpose-driven, but also operates a lot like a start-up and operates on the basis of trying to understand what outcome it can achieve before it starts doing things.

Tech Against Terrorism is a very small, lean organization. I set out trying to create a small not-for-profit that behaved like a start-up and was incredibly focused on building technology, using technology well, and trying to cut through the noise that often comes with very large, bureaucratic initiatives that governments and large companies are involved with. What I wanted to create was the antithesis of a normal public-private partnership, the antithesis of a normal not-for-profit, an organization focused on operational impact first and foremost. This ethos, I'd like to think, has been a large part of why Tech Against Terrorism has been extraordinarily successful despite being a very small team with very limited funding. And to be clear, I don't want a bigger team. I don't want more funding. The fact that we have this limited budget and limited team size forces us to be more thoughtful about how we can be effective. It's a paradox with organizations that the bigger you get, the less effective you become. With Tech Against Terrorism, being lean is an essential part of our effectiveness.

^a Editor's Note: Tech Against Terrorism and QuantSpark were founded in 2016.

CTC: A central part of Tech Against Terrorism's work is the development of tools such as the Terrorist Content Analytics Platform (TCAP). Can you share a bit about Tech Against Terrorism's core tools, who uses them, and their practical real-world value?

Hadley: Tech Against Terrorism is not just focused on working with tech platforms to improve content moderation with regards to terrorist content but also trying to understand how we can use and deploy technology to do it. We have a small engineering team that builds tools, and the Terrorist Content Analytics Platform is one of them. It provides enormous value to hundreds of platforms and is a very simple idea well implemented, which is to support the workflow of our open-source intelligence analysts, speed up the verification of terrorist content, and then alert platforms. Over time, what we've done is built in various tools to archive this material, to hash this material, and to feed this into an automated pipeline of processing leading to alerts, hashing, and archiving. The Terrorist Content Analytics Platform essentially serves to help report verified examples of terrorist content created by organizations that have been designated as terrorist organizations in the U.S. It's a very high threshold for reporting content created by actual terrorists. Through doing this, we've reported hundreds of thousands of pieces of content across the internet, and this is going from strength to strength as we're building out a network of trusted flaggers who can help expand the aperture of this intelligence collection activity.

In addition to this, we're building tools using generative AI, using large language models to determine when content has been removed because we want to understand which platforms need more support or maybe where there's ambiguity or where terrorists are particularly congregating online. We use technology all the time not to replace what we do—human-in-the-loop^b integration of AI is very important—but to increase the productivity of our team by 10x, which means that whilst we may only have a team of five to 10 people, we're as productive as you might expect from 50 or 100. We also use this technology not only to collect intelligence on where terrorist content is, but to summarize this activity, to analyze this activity, and to produce intelligence assessment products for our stakeholders and partners.

CTC: Can you tell us a little bit about your work at QuantSpark and synergies that might exist between your role there and your role at Tech Against Terrorism?

Hadley: Having the ability to tap into a deep expertise in terms of software engineering, data science, and AI is certainly very helpful. Tech Against Terrorism and QuantSpark are separate entities, but certainly Tech Against Terrorism wouldn't have survived this long were it solely relying on government grants and tech companies. The fact that we've had access to an almost pro bono pool of technical specialists has meant that Tech Against Terrorism has been able to punch above its weight technically. Were we to try and do this at commercial day rates and go to market, it simply would

not have been viable.

Long gone are the days when you could just have conferences or just have reports or just have research. You've got to build software these days, even as a not-for-profit. Your primary activity should be building software because, let's face it, the only way you're going to have impact in the world—especially when you're dealing with technology—is if you yourself are a technologist and using technology to have that degree of impact. When I look around the community and look around the space, I wonder if only more people were product managers, if more people had experience building software, we'd be much more productive as a sector.

CTC: With the work that you do at QuantSpark and Tech Against Terrorism, it gives you a unique vantage point of the field. In efforts to combat terrorist use of the internet or online activity, if you had to evaluate the field and community of practice that's focusing on this area, where has it performed well? What are its problems or core challenges? And where does it need to improve?

Hadley: This might sound like a strange thing to say considering I've been doing this for more than a decade, but I still feel like an outsider from the counterterrorism community. Whether that's about me or about the community or something else, I'm not sure. But having a slightly different perspective means that it's a bit easier to see where there are opportunities to do things better. We've got to focus on outcomes first and work backwards. This requires rigorous critical reasoning and analytical faculties and the application of intelligence assessment techniques. Counterterrorism is a space that is quite contested as well, with a very large amount of academic and research interest. This will be a controversial thing to say, but I don't think counterterrorism is a single academic discipline. I think it's quite a complex discipline that involves psychology, sociology, criminology, theology, and all these other 'ologies.'

Now, in terms of what the community could do better, we've all got to acknowledge the fact that counterterrorism is no longer a popular pursuit politically. And terrorists often benefit from complacency. Right now, of course, counterterrorism has been comprehensively defunded within governments, within tech companies. Only last week, a major government counterterrorism team was just fired.¹ At tech companies, this is not a major focus anymore. Yet, regrettably, if we look at the statistics in terms of the prevalence of terrorist content online, it's abundantly clear that terrorist activity has returned with a vengeance on the internet, even though probably the kinetic threat to the U.S. and the U.K. and E.U. is lower than it has been for a while. The use of the internet by terrorist groups operating in other parts of the world has never been higher, and the destabilizing impacts of terrorist groups in Africa, Central Asia, the Middle East, Southeast Asia is peaking. So, I think there is a strategic confusion—I would say in the U.S., in Europe, in the U.K.—that there are just so many state threats and non-state threats for policymakers to digest that counterterrorism has basically, in my view, been completely forgotten. The community is under threat from complacency. It needs to get better at articulating the nature of that threat, and you could argue that this is an overcorrection from a few years ago when there were simply too many people in the counterterrorism space. So, the first thing I would say is there is a risk in my opinion of overcorrecting and there being almost zero capacity to look at over-the-horizon threats

^b Editor's Note: "Human-in-the-loop (HITL) machine learning is a collaborative approach that integrates human input and expertise into the lifecycle of machine learning (ML) and artificial intelligence systems." "Topics: Human in the Loop," Google Cloud, accessed July 15, 2025.



Adam Hadley

where terrorism is concerned.

I do think we've lost focus as a community, and we need to refocus on the most egregious threats. And this is a rather crude word, but we need to think about return on investment. We need to think about what our objectives are and how we evidence this. At Tech Against Terrorism, we have an abundance of evidence: content removal, disruption of terrorist-operated websites, and increasingly disruption of live terrorist attacks and threat to life. So, in summary, I would say broadly that the policy-making community has lost interest in counterterrorism and that is a strategic error, but at the same time, the community hasn't helped itself by losing focus and forgetting to work backwards from the intended outcomes.

CTC: Do you think that part of the challenge in the counterterrorism space, particularly when it comes to terrorist use of digital technologies, is just the fragmentation of the landscape, of the different equities that different players have, whether that's government or platforms themselves or those that operate outside of those areas? When I look at the community and the landscape, there are a lot of solutions, and it could be so much more powerful if there was more collaboration in areas where that collaboration made sense. Do you feel the same?

Hadley: Answering that backwards, I'd say that the word 'collaboration' or 'public-private partnerships' are often used quite loosely. We also have to recognize that as a community, there's an extraordinary amount of competition. I run a for-profit company, QuantSpark. I run a not-for-profit NGO Tech Against Terrorism. And I must say, the environment that Tech Against Terrorism operates in is significantly more competitive than a private company. It's a lot less collaborative than the private sector. It's in some ways more ruthless. Especially when funding is so restricted,

it's very easy for people in the community to undermine one another by accident. We as a community need to get a lot better at focusing on what we're trying to achieve, and it might be sometimes *not* doing a project because someone else is better at it. Or it might be collaborating. Part of that is the dynamics of this community, and I largely hold funders responsible for this where funders often don't really know enough about the area and fund conflicting programs of activity and don't focus on synergy. And the reason for that is geopolitical: Countries don't want to collaborate. They want to be seen to be doing things. Often, the problem starts because funders want talking points, and that can cause a lot of inefficiency in terms of delivery.

You could argue that the word 'fragmentation' is the word of the decade. We have a fragmented political landscape—internationally, domestically—fragmented technology and tech stack. Certainly, the fragmentation of terrorists to the internet is a function of adversarial shift, which in a sense is a sign that we've all been doing some good stuff. A lot of the low-hanging fruit has already been disrupted, apart from terrorist-operated websites, which is more like 'back to the future.' But a challenge that we're all facing in many disciplines is that the technical complexity of what we're trying to do is increasing faster than our ability as professionals to learn the new technologies. It's almost like technology is alienating ourselves from our own disciplines, and therefore, you might be an expert in counterterrorism and you may be steeped in the theology of a particular organization or the ideology of an organization, but how on Earth can you keep up with the exponential growth created by generative AI? I think *that*, singly, is the bigger challenge we all face as knowledge professionals: How can we keep up with this terrifying pace of technological progress? This is more generally a problem with generative AI. Technology is racing ahead of humanity, and the experts are struggling to keep up.

CTC: It's interesting to hear your comment previously about feeling like an outsider in the counterterrorism field. Because what you just mentioned about the complexity, if you project forward, it really seems as though organizations like Tech Against Terrorism that are trying to bridge the gap and create synergies between social sciences approaches and more technical physical science approaches, computer science, leveraging technology, that's the way we're going to get a better handle on this complexity.

Hadley: The nature of complexity is something we *all* need to be thinking about more and so-called wicked problems.² There are so many more wicked problems we have to deal with now, without almost recognizing them as such. Part of this is that quite a few traditional ways of working—let's say in the intelligence community or the counterterrorism community or in government in general—themselves need to be disrupted. This seeming cultural aversion to open-source intelligence is part of the problem. This almost obsession with secret intelligence may have made sense pre-AI, but we're now approaching a singularity where it's possible to gather such a vast array of data, publicly available or commercially available data, that when you combine that with fairly basic approaches and techniques with large language models and agentic AI—again, another controversial thing potentially to say—the entire intelligence enterprise is ripe for disruption. The combination of gathering very large amounts of data and treating it with AI is so

formidable, but there's so much cultural resistance to this that that's the biggest barrier to adoption for technology. It's not actually the technology, but rather change management, fear of the unknown, and individuals perhaps being slightly frightened of things they don't understand.

All of us as professionals need to recognize that our knowledge will become irrelevant and useless more quickly than ever before, that our own kind of utility as knowledge professionals is atrophying with an increasingly limited or short half-life. The way forward really is for all of us to focus on not just keeping up with the news about technology but also embracing studying the application of AI and how to build software that applies this. I firmly believe that pretty much in every discipline, the primary way you're going to have impact is by coding. It's by building software, which is such a radical shift from what we are used to. And generative AI is making it much more accessible as well. You don't really need to be a coder anymore to build software; you just need to have a good idea and access to generative AI tools that can help you prototype software quickly. So, I'm rather hoping that the expertise and creativity that we have in the community can be applied in a more practical and operational sense with regards to software development, because that's really going to be the only way we can deal with the complexity.

Unless we vastly accelerate the pace of our own understanding in this area, hostile nation-states will overtake us, and the more sophisticated terrorist organizations will as well. It is a race against time. It behooves all of us to promote education in this space because there is a very real risk as we go into quite a dangerous geopolitical era that our generals and our policymakers are thinking about bombs and bullets³ instead of bytes and bits.

CTC: When it comes to terrorist use of technology and online aspects, what trends or use cases concern you the most? Which do you feel are underappreciated in our community?

Hadley: There are two sides to this. One is, there are push and pull factors. What theoretically could terrorists do? What do they actually do? And what explains the gap between the two? There are lots of things that terrorists *could* be doing, but they appear not to be. A lot of the conversation is about the emerging threats. That's relevant, I suppose, because it's novel, it's new, it's interesting, and we all like to think about the new and the novel. But the reality is the terrorists' use of the internet is pretty similar to what it has been for quite a long time. And yes, there are some qualitative improvements to how they're using technology to produce content, but we haven't seen a big shift with AI.

What I would say is, probably the most concerning trend—which is still very low baseline—is the increased personalization of content for radicalization and mobilization journeys. However, this is still 0.01 percent of activity. Most of the terrorist activity online is quite simple, quite rudimentary. It's sharing content, it's having conversation, it's looking for bomb-making materials, it's doing basic ISR work. An example of this is terrorist-operated websites. We're tracking 400 websites that we assess all of them to be almost certainly owned or operated by a designated terrorist organization. This is terabytes of freely accessible information online, and very little is being done about it. So, there's a lot of hue and cry about AI, but when it comes down to it, the basics have been forgotten. The debate about generative AI seems to be to the exclusion of focusing on common sense, which is terrorist-operated websites and the

“Unless we vastly accelerate the pace of our own understanding [of AI tools], hostile nation-states will overtake us, and the more sophisticated terrorist organizations will as well. It is a race against time. It behooves all of us to promote education in this space because there is a very real risk as we go into quite a dangerous geopolitical era that our generals and our policymakers are thinking about bombs and bullets instead of bytes and bits.”

sharing of obvious content on major social media platforms. So, yes, the trend is towards more personalized content. Generative AI can help that. The trend you've outlined is towards fragmentation across a greater number of platforms, but fundamentally not a lot has changed. We just need to remain alert to terrorists following the path of least resistance.

Not wanting to contradict myself, but one big threat down the line is the use of agentic AI. This is when it becomes easy to create your own bots where you can create your own distributed network of 10,000 social media profiles, posting nonsense and doing so automatically. The barrier to entry for the more technical work is being lowered both for us as specialists in this area but also for terrorists, which means that the use of agentic AI and circumvention techniques to create tens of thousands of accounts online and create terrorist content with abundance is not so far away. We must hope that the major platforms are a few steps ahead and are using generative AI to get ahead of the threat. Because unfortunately, the future is one in which we have many orders of magnitude more content on the internet and many orders of magnitude less authentic content on the internet. And that applies to terrorist content and disinformation.

The final thing I'll say on this in terms of emerging threat is not actually about the terrorist use of the internet, but the increased convolution of hostile nation-state activity online and the role that terrorist content may or may not play in that. Many of our nation-state adversaries are quite opportunistic. Many of them are very thoughtful and within their published doctrine include information operations. Now obviously in the West—in the U.S., in the U.K., in the E.U.—the information environment is largely completely ignored. I suppose the extent to which traditional military think about information operations is dropping fliers from aircraft. It's embarrassingly primitive, but adversaries have information operations at the core of their own military doctrine. As a result of this, we are seeing examples in the public domain of hostile nation-states encouraging terrorist acts, encouraging polarization, creating fake networks of terrorist content. So, talking about the complexity, it's not just about the technology, it's also about the operating environment, where it's going to become increasingly difficult to

distinguish between a nation-state actor pretending to be a terrorist and a terrorist being supported by a nation-state actor. It's going to become much more ambiguous and gray. I think with the specter of hybrid warfare we are experiencing right now, I worry that our doctrine, our investment, our technology, our policy focus is simply not equipped to deal with that degree of ambiguity.

CTC: Speaking of hybrid warfare, we don't hear a lot about the Houthis' online presence and their use of digital platforms and technologies. In prior conversations, the Tech Against Terrorism team has mentioned that the issue deserves more attention. Can you unpack that a little bit?

Hadley: The Houthis have certainly surprised the counterterrorism community with their military ingenuity, but despite their tenacious efforts attacking Israel from Yemen, their kinetic impact remains pretty limited. What demands attention is their full spectrum media strategy across social media and their own websites; they're not trying to terrorize but rather tap into anti-Israel domestic sentiment and shore up their own political support. Their use of the internet also represents a significant intelligence collection opportunity that we're simply not exploiting. Their overarching objective is recognition and international legitimacy as they aspire to control Yemen, which means their military actions are as much about symbolic projection of power as they are about military effect. Here's the glaring contradiction: Whilst they're designated as a Foreign Terrorist Organization under U.S. law, the Houthis operate completely uncontested across digital platforms, producing sophisticated propaganda that directly supports their strategic goals. We're not just missing an opportunity by ignoring the information environment; we're fundamentally misunderstanding how kinetic operations can undermine strategic intent when their propaganda machine transforms every strike into a recruitment tool and legitimacy claim. Since their online information operations are so aligned with their military activity—both serving the same strategic goal of projecting legitimacy—this represents a profound strategic misunderstanding of how to counter organizations like the Houthis. We're ceding the information domain whilst pursuing kinetic solutions that feed directly into their narrative, which shows we've failed to grasp the very nature of this conflict.

This applies to al-Shabaab as much as anyone else. Al-Shabaab's internet activity is one of the most prolific of all terrorist organizations with vast global reach, extensive financial networks, and connections to diaspora communities worldwide. Yet senior policymakers in military and foreign affairs circles seem to completely ignore hybrid warfare as a concept with regards to the terrorist use of the internet. The moment hot conflicts erupted in various parts of the world, everyone forgot about hybrid warfare and the critical role the information environment plays within it. Here's a provocative question: What proportion of defense spending goes on understanding and disrupting the information environment? Is it one percent? A tenth of one percent? A hundredth of one percent? I don't know what it is, but I know it should be significantly more than it currently is. What I do know is that in any serious hostilities, the information environment would be the first battleground—and probably the first one we'd lose.

CTC: You talked about generative AI and AI and terrorism. Specifically related to counterterrorism, what are some of the

more important and most interesting use cases that you've come across in that area, and what more needs to be done?

Hadley: I'd split this into three separate buckets. The first is generative AI as a force multiplier for an individual analyst. The second is thinking through generative AI to supercharge organizational processes. And the third is emergent use cases that would never have been possible previously. So, the first one is as an individual analyst or researcher, off-the-shelf generative AI tools when used well, can and do increase productivity, when summarizing content, translating content, extracting information from content. I'm sure many of your readers have spent days upon days transcribing material or coding text or extracting information from screenshots or PDFs; you could argue 90 percent of time doing research historically has been manual grunt work. All of that can be done in milliseconds now, where you can just throw primary research at large language models and you can just structure information and extract information. That's a massive force multiplier. That's already 10x to a good analyst or good researcher, whether in government, academia, or tech companies. There's a misnomer that generative AI is about generating output. Generative AI is good at transforming one format of information to another format of information. So, the primary benefit to all of us now is getting this technology used in our day-to-day workflows as researchers and as analysts. For instance, if you're an intelligence assessment professional, you can even use generative AI to support analytical techniques such as Analysis of Competing Hypotheses (ACH) or you can draft a Cone of Plausibility in seconds, whereas historically that would have taken you days to do and therefore wouldn't have been done in an operational environment.

That's the first wave of things: analysts getting more comfortable using this technology and being allowed to use it and stopping laggards in bureaucracies from stopping the adoption of this technology because there are very safe ways of using large language models. There are open-source, large language models like Llama that you can install locally in an air-gapped environment. So, a lot of the concerns about privacy, about information exfiltration are, in my opinion, overblown and are stopping analysts using this amazing technology, which means that government circles are way behind the private sector, and they're way behind our adversaries.

The second is about workflow. Generative AI is useful to bridge the gaps between systems, to translate information from one type to another, to convert handwritten notes or voice notes into something. A lot of operational processes in the police, intelligence, and wherever is essentially a web of different processes, and generative AI can sit above all of this and fill in the gaps and accelerate existing processes, especially when you're triaging radicalization or mobilization leads. So, especially in the threat space, generative AI can vastly reduce the burden of form-filling and connecting one system to another because it can connect all these things up.

The third is what I call emergent use cases, particularly using agentic AI, where you have a large language model that has its own thought process so it can manage other agents or other technologies. It's almost a metaphysical layer of abstraction above technology where you can get AI to orchestrate other technologies and instruct other tools and technologies to do things. What this means is you can have hundreds, if not thousands of 'workers.' Give it a couple of years and you could probably get an agentic system to do the work of 400 people, provided you are able to describe their

“My hope comes from the fact that the sophistication of the new technologies that are emerging is so great that despite the inertia and lack of focus, the technology will be so powerful that it will provide several orders of magnitude more productivity. My hope is that the scale and the power of generative AI and the data sets that are increasingly available and the ease with which it is possible to build technology to counter terrorism will make up for any deficits and deficiencies in the current counterterrorism landscape.”

work clearly enough that it could be delegated. Therefore, a lot of AI adoption is about being very good at delegation. It's trying to explain how to solve a problem clearly with enough context and clarity that an AI can replace that particular process. The third wave is truly mind-bogglingly exciting. If you know how to design these systems and have an abundance of imagination and experience and contextual understanding, you could build an analytical system that could replace 400 analysts. This is potentially extremely interesting with regards to triaging content at scale, in order to find threat to life indicators or even radicalization indicators. If you can get an AI system to do something 80 percent as well as an intern but you can have tens of thousands of them, you then have emergent capability that's unlike anything you have seen previously. That's very hard for people to get their head around because as humans, we believe that a tool must be 99 percent as effective as a human. It doesn't. It needs to be a bit better than an intern. But at scale, it can be incredibly powerful. That's the third wave, which is probably a few years away. I very much doubt government is going to support that sort of work. I'd imagine that innovation will come from the private sector.

CTC: You've talked about how various parts of intelligence process are ripe for disruption, how governments are behind, and the different risks and cultural factors that shape adoption of AI. And then, we have the speed of AI and how things are moving. Do you think that governments are too far behind given where this is going?

Hadley: Yes, undoubtedly. But you never entirely know what's going on inside governments. So, there may well be islands of secret innovation, but certainly, I would sincerely doubt that governments have progressed particularly far. I think it's a combination of lack of funding, lack of imagination, and excessive caution with regards to the legal infrastructure. And in America, you don't really have

GDPR or RIPA.^c Part of the problem with the internet is going on someone's social media profile in some circumstances is considered legally equivalent to in-person surveillance in someone's garden. So, the legal infrastructure is, in my view, really backwards. And what this does is create a climate of inertia. And let's face it, government is already inertial. But combined with this fear about AI, fear about the internet, fear about conducting surveillance, it's a somewhat toxic formula, which is militating against innovation in this space at the very time that we need government to be doing more. And the fact that so many of the leading NGOs in this space are almost bankrupt suggests that there isn't really funding to solve these problems; that many of the social problems we're facing, there aren't many companies prepared to invest in that. There aren't many corporate philanthropists anymore. There aren't many businesses that are prepared to pay to solve the social problems that they help create. So, there is a market failure here as well; I don't think we can assume that the private sector will pick up all the slack.

CTC: When you look out over the horizon and think about how the intersection between terrorism and technology is going to evolve, what concerns you and what gives you hope?

Hadley: What concerns me is that in the absence of a recent major terrorist attack in the West, we've lost leadership. It seems to me that the only way, unfortunately, that this community can focus is through tragedy, and I really hope that we're able to focus based on an objective appreciation of the threat, on things that matter. We shouldn't have to wait for a big terrorist attack to start thinking about counterterrorism. I fear that that is inevitable, that the community will only focus after the next attack, by which point it would be too late.

My hope comes from the fact that the sophistication of the new technologies that are emerging is so great that despite the inertia and lack of focus, the technology will be so powerful that it will provide several orders of magnitude more productivity. My hope is that the scale and the power of generative AI and the data sets that are increasingly available and the ease with which it is possible to build technology to counter terrorism will make up for any deficits and deficiencies in the current counterterrorism landscape.

CTC: Is there anything that we haven't talked about that you want to cover?

Hadley: The key thing is that when countering terrorists, we have to uphold the fundamental values in our society. This is an ethical position, but it's also a pragmatic one because if we dilute our standards, then we let the terrorists win. What the terrorists want really, and what many nation-states want as well, is to undermine

^c Editor's Note: "The General Data Protection Regulation, or GDPR, is a European Union (EU) law that governs how organizations within and outside the EU handle the personal data of EU residents. GDPR was adopted by the European Parliament and Council of the EU in 2016 and took effect on 25 May 2018." "What is the General Data Protection Regulation (GDPR)?" IBM, accessed July 15, 2025. The Regulation of Investigatory Powers Act 2000 (RIPA) is U.K. legislation that governs the use of surveillance and investigatory powers by public bodies. It was enacted to ensure that such powers are exercised in a manner compatible with the European Convention on Human Rights, particularly the right to privacy. See "Regulation of Investigatory Powers Act 2000 (RIPA)," U.K. Home Office, updated July 25, 2025.

our collective security and stability and our effectiveness as democracies. In designing counterterrorism programs, respect for human rights and fundamental freedoms—the U.S. Constitution, for instance—is not a nice-to-have; it’s a necessity. Otherwise, it undermines everything we are doing from a moral and practical standpoint. We’ve got to make sure that we don’t dismiss parts of counterterrorism that have become a bit distracted by non-core terrorism issues.

And we’ve got to make sure that policymakers in companies and in government don’t dismantle counterterrorism for political

purposes, because if they do, we know that terrorists will rebound. There are many areas of contestation in the world, the Sahel, North Africa is one of these areas where there is, without a doubt, state collapse across many countries. It’s easy to imagine a world in which we have another Afghanistan, in the Sahel, at a time when governments have lost focus and tech companies are not being held to account. We’ve got to focus on the threat; we’ve got to focus on the hard counterterrorism work before it’s too late. **CTC**

Citations

- 1 Editor’s Note: See Jory Heckman, “State Dept lays off 1,350 employees as reorganization nears final phase,” Federal News Network, July 11, 2025.
- 2 Editor’s Note: As defined in Horst W.J. Rittel and Melvin M. Webber, “*Dilemmas in a General Theory of Planning*,” *Policy Sciences* 4:2 (1973): pp. 155-169.

- 3 Editor’s Note: See Adam Hadley, “We Need to Move Beyond Bombs and Bullets to Counter Terrorism,” RUSI, September 6, 2024.