CONVERSATIONS ON STRATEGY

PODCAST TRANSCRIPT

COL Eric Hartunian and LTC Paul Milas On *Emerging Technologies and Terrorism: An American Perspective*

Colonel Eric Hartunian and Lieutenant Colonel Paul Milas, co-editors with Susan Sims of *Emerging Technologies and Terrorism: An American Perspective*, discuss their newly published collaborative study from the US Army War College Press. The publication focuses on how terrorists may exploit emerging technologies such as artificial intelligence, autonomous systems, augmented reality, biotechnology, and nanotechnology from an American and Western Hemisphere perspective over the next 5–10 years. They highlight the pace of technological development and the need to safeguard against terrorist exploitation of these innovations.

Keywords: artificial Intelligence, AI, drones, nanotechnology, agriculture, augmented reality

E-mail usarmy.carlisle.awc.mbx.parameters@army.mil to give feedback on this podcast or the collaborative study.

Stephanie Crider (Host)

You're listening to Conversations on Strategy.

The views and opinions expressed in this podcast are those of the authors and are not necessarily those of the Department of the Army, the US Army War College, or any other agency of the US government.

Joining me in the studio today are Colonel Eric Hartunian and Lieutenant Colonel Paul Milas, coeditors with Susan Sims of *Emerging Technologies and Terrorism: An American Perspective*.

Hartunian is the director of the Strategic Research and Analysis Department in the Strategic Studies Institute at the US Army War College.

Milas is the Director of African Affairs at the Strategic Studies Institute at the US Army War College.

The topic of discussion is *Emerging Technologies and Terrorism: An American Perspective*, which was published by the US Army War College Press in May 2024.

Congratulations. Tell me about the collaborative study .

Lieutenant Colonel Paul Milas

Thank you, Stephanie.

We began working on this project in early 2023 in partnership with the Center of Excellence Defense Against Terrorism, or COE-DAT.

COE-DAT is a NATO-accredited multinational organization in Ankara, Turkey, that provides NATO and partner nations with a comprehensive understanding of terrorism and counterterrorism-related challenges. This book is the second part of a two-part study sponsored by COE-DAT that examines emerging technologies in terrorism over the next five- to 10-year time span.

The first book, which published in 2022 by COE-DAT, focused on emerging threats from an Asia, European, and Middle East perspective, while this book examines how terrorists may use emerging technologies over the next 5–10 years from an American and Western Hemisphere perspective.

Over the past year, we organized a series of workshops bringing together experts in terrorism and emerging technologies and asked them to forecast how terrorists could potentially exploit emerging technologies over the next

five- to 10-year time frame. We intentionally left the door open without confining our authors to any specific threats or technologies, and we didn't try to narrowly scope their research. So they were free to explore all possibilities and be creative with their research.

The authors identified several technologies that could be susceptible to terrorist exploitation to include artificial intelligence, autonomous systems, augmented reality, biotechnology, and nanotechnology. And that's really what our book is framed around, those five technologies.

Getting back to the question of why are we publishing this book now—technology is developing at an incredible pace, and many of these cutting-edge technologies are increasingly available to the general public. Technologies such as artificial intelligence, autonomous systems, and augmented reality have become part of our everyday lives. And some of us use these technologies every day. And these include things like chat GPT, drones, Apple Vision Pro, and self-driving cars.

While these technologies are generally intended for good purposes, terrorists are finding ways to exploit these same innovations for their own sinister purposes. And the line between reality and what used to be science fiction is blurring. And in many cases, we lack safeguards against these technologies. And these technologies are getting into the hands of terrorist organizations.

So, the time is right to craft solutions and safeguard technologies and prevent terrorists from harming the public with these technologies and misuse.

What does this all mean, and where do we go from here?

Colonel Eric Hartunian

Thanks, Paul. So, the first thing I want to talk about is to frame this discussion around three themes: size, accessibility, and attribution.

When we're talking about size in emerging technologies, the first thing we need to realize is that we're really talking about things that are microscopic in size. We're talking about nanometers. So, if you think about a human hair, that's about 80,000 nanometers thick. A particle of DNA is about two-and-a-half nanometers. One cell of bacteria is about 1,000 nanometers. Particles this size, they can't be detected by optical microscopes.

If you think about the US in a post-911 world and airports all over the country that are staffed with [Transportation Security Administration or] TSA agents to detect dangerous things that could come onto an airplane for a terrorist attack, there's nothing that those agents have that can identify the kind of technologies that we're talking about in this case. They're simply too small.

The second aspect that I want to talk about is accessibility. Now, we're not talking about access to specific conventional weapons in this case. Even most weapons-grade [weapons of mass destruction or] WMD is relatively difficult to get, and we generally have policy tools and regulatory frameworks that monitor those kinds of items and the precursor materials that go into making them. So, while the thought of a nuclear weapon in the hands of a terrorist is indeed terrifying, access to that kind of weapon isn't really easy. But when we talk about the kind of emerging technologies in this study, we're seeing a much lower barrier to entry, both in terms of finances and access to the technology.

So consider cheap, small drones that are readily available online, often for under $100 in the US, and they're really easily weaponized. And we're seeing that in Ukraine. We're seeing that in Israel. These take almost no training to fly, and they're actually quite capable machines. Or we can also consider AI technology. It's often free online or at a minimal subscription cost. Or an individual with little to no training can quickly generate a deepfake video and post them online for ill intent. So, the democratization of this technology, while it's amazing in some respects, it really presents significant risks for the [counterterrorism or] CT community.

And then lastly, I want to talk about attribution. In most terror attacks, our response is often governed by our ability to attribute blame, whether that's to a group or to an individual or to a state. So, the small and accessible world of these new technologies really creates significant roadblocks to our ability to attribute these attacks to other perpetrators. In some cases, some of these attacks could be on food supplies or they could be against genetic manipulation that targets specific populations. The terror attacks of the future may not even be recognizable as attacks until long after the damage is done and the attack's over. So even then, if the attacking party does not claim responsibility, attribution will limit our ability to respond significantly to the event.

So, with these themes as a backdrop, I'll talk a little bit more specifically about the project and how we categorize these threats into four brief categories that I'll go into right now. First is we have the idea of invisible visible extinction. So here, again, size matters. And as I previously said, we're talking about nanometers. These are genetic mutations and particles that can target specific individuals or whole groups of people. They can target brain functions to cause a cardiac arrest. These are weapons that are virtually undetectable, and they can act immediately, or they can have a delayed response. An attribution in this case will be almost impossible.

The second is unmanned killing machines. Think about unmanned devices that are increasingly accessible, available, and cheap. They're getting smaller, they're able to fly farther and faster, and they can carry heavier payloads. We've all been seeing these devices in action in Ukraine, as I stated previously, and how they're doing more on a less conventional battlefield.

So how can these be used?

In the agricultural sector, we can, you know, drones can be used to map fields, they deliver pesticides and fertilizers. So, it wouldn't be out of place or cause any alarm if you saw drones circling above a small or a large farm.

The increasing ease with which these drones can be weaponized with harmful agents is really worrisome because people won't even realize that what they're seeing is, in fact, a terror attack happening. Drones and self-driving vehicles can be loaded with explosives or chemical or biological weapons. They can be used to target crowds or critical infrastructure. They can destroy crops or contaminate water supplies. They can even be controlled by AI, further challenging the ability to attribute responsibility for whatever they devastate.

And then finally, we have when virtual becomes real. We're seeing lots of opportunities where virtual reality is becoming ever-present in our modern lives. Terrorists can harness your biometrics, face, retina, iris, your ear shapes, your palm, your fingerprints, voice patterns, all of that from you TikTok videos to hack into secure systems. They can create dummy eyes or 3 - D print faces of government officials from photos on websites. Chatbots can be used to identify and recruit vulnerable individuals and plan attacks. Augmented reality can create realistic, persuasive environments for radicalization, even for mission planning and execution.

These are all areas where the virtual world can be used for terror attacks.

Milas

Can you give me an example?

Hartunian

Yeah. So, one of our researchers used a subscription-based service, which was under $20 a month, to create videos that demonstrated how a single individual could radicalize masses using a virtual meeting space and then use that meeting space to train individuals to conduct attacks and then to use that same meeting space as a way to collaborate and direct an operative to go out and conduct an attack. This was done with about, like I said, almost virtually free technology that's available online. And the person who created these videos had no training to do it. So, he was able to conduct that really with just a little bit of an imagination and the ability to put it together on a virtually free online platform.

COL Eric Hartunian and LTC Paul Milas On *Emerging Technologies and Terrorism: An American Perspective*

Milas

What kind of recommendations would you suggest?

Hartunian

So, I think we have only a few recommendations to go off of here. Unfortunately, this is an area where I think we're always going to be chasing our tail. The idea that we'll ever be able to get out in front of this is something that's not terribly realistic right now.

But I think we have a few areas where we can do some good. First, I think we need to really work on improving policymaker knowledge. One of the ways that we can do this is to put specialists, whether they're scientists or academics or people that are practitioners with some of these technologies, in the same room with policymakers so that they know what to regulate. Right now, I think our regulatory frameworks, they're a patchwork between nations and between states, and I don't think that there's enough overlap to catch these kinds of would-be terrorists using these kinds of technologies.

The second thing I think we really need to work on is developing a better sense of imagination. We have so many new technologies coming on the landscape where most of them, are really intended for positive outcomes and to help society. But it really doesn't take much for somebody who wishes ill to use those same technologies and find ways to employ them in nefarious ways that can cause really devastating results from a terrorist perspective. So, I think that sense of imagination is something that we need to foster and be able to use to create the right kind of policies and regulatory frameworks that can help us get after some of these technologies and prevent them from being used in ill ways.

Milas

One of the things that surprised me the most with this research is the ease of which these technologies could be adapted by terrorists. While a lot of these technologies like AI and autonomous systems are very complex, and a lot of the big tech companies are having a difficult time developing these, so it's certainly going to be even more difficult for terrorist organizations.

What surprised me was the relative ease and the potential use to manipulate the existing technologies, things like drones and autonomous systems being able to be hacked into versus being developed.

As Colonel Hartunian said, drones in the agricultural industry already exist. The potential for those to be adapted by terrorist organizations is relatively easy, and that's probably what surprised me the most with what came out of this project.

Hartunian

Right. So when we think about what we do about those kinds of things, we need to consider how do we alert and make aware our populations without alarming them too much. Because we don't want people running around terrified all the time, but at the same time, we need people to understand that there are threats out there, and they could come in the form that we're talking about is in a technology that they use in their daily lives.

Host

Do you have any other concluding thoughts you want to share about this?

Milas

I would like to thank our authors and our contributors to this project, and a special thanks to COE-DAT, who sponsored this project and this work.

Thank you.

COL Eric Hartunian and LTC Paul Milas On *Emerging Technologies and Terrorism: An American Perspective*

Host

Are you working on anything else that our listeners could look forward to?

Hartunian

Continuing this theme of emerging technologies. Over the course of the next year, one of our researchers, Dr. Tony Pfaff, is working with NATO's COE-DAT to develop a project focused on the use of AI and AI technologies in terrorism and how that can be another area where the [counterterrorism or] CT community needs to come together and determine how they're going to get in front of and deal with that threat.

Host

Listeners, you can find the monograph at press.armywarcollege.edu/monographs.

For more Army War College podcasts, check out Decisive Point, SSI Live, and A Better Peace.

Eric, Paul, thank you so much. This was very interesting.

Milas

You're welcome.

Hartunian

Thank you.

Download this episode:

https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Conversations-on-Strategy-Podcast/mod/67381/player/581/audio/81290