A View from the CT Foxhole: Christopher Maier, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

By Sean Morrow, Don Rassler, and Kristina Hummel

Christopher P. Maier is the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Among his responsibilities are all special operations, irregular warfare, counterterrorism, and information operations policy issues and the oversight of special operations peculiar administrative matters, on behalf of the Secretary. He previously led the Department of Defense's Defeat-ISIS Task Force from its inception until disestablishment, charged with policy and strategy development, international negotiations, oversight, authorities review, and national-level interagency implementation of the Department's role in the U.S. government's campaign to achieve an enduring defeat of ISIS. In this role, he also directed the Secretary of Defense's leadership of the Defense Ministry components of the 80+ international members of the Defeat-ISIS Coalition.

From July 2015 to September 2017, Maier served as the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism. Before moving to the Department of Defense, Mr. Maier held several positions at the National Counterterrorism Center (NCTC), including Senior Advisor to the Director, Chief of Strategic Assessments and Regional Planning, and Chief of Staff in the Directorate of Strategic Operational Planning. From 2009 to 2013, Maier served on the National Security Council Staff as a director for counterterrorism.

CTC: Many of our readers will be familiar with the function and role played by the ASD SO/LIC team, but some of our readers may be less familiar. Could you provide a brief overview of your position, the role of your office and your team, how CT fits into it, and some of the key initiatives that you're working on?

Maier: SO/LIC came about the time the U.S. Special Operations Command was stood up in 1987, and it was meant to be the civilian arm of it to provide oversight. It is the original assistant secretary-ship that Congress created.

SO/LIC has evolved, especially in the last six years, to be more than just a policy organization. The ASD and the deputy assistant secretaries support the Under Secretary for Policy across a range of issues such as counterterrorism [CT], counternarcotics and now, information operations, and stabilization in various forms.

SO/LIC's service secretary-like role is akin to what the Army, Navy, and Air Force have on the uniformed side. Now, SO/LIC doesn't have the same comprehensive set of authorities over the Special Operations enterprise, but what has really changed in the last six years or so is that Congress has progressively strengthened the service secretary role.

The ASD SO/LIC is in the chain of command for the administrative oversight of Special Operations Command. What that means is Special Operations Command is both a Title 10 Combatant Command, much like Central Command or European Command is, with operational authorities directly to the Secretary of Defense, but also has a unique role focused on the organizing, training, and equipping Special Operations Forces [SOF] across all the services.

As ASD SO/LIC, I have the civilian oversight of that organize, train, and equip role and report directly to the Secretary of Defense while still serving as the senior advisor to the Under Secretary for Policy on all SOF and low-intensity conflict issues.

It's a bit of an unusual organization within the Department to have a dual reporting chain with two different jobs. But what I see as the value of that is we can figure out on the policy side what it is we should be doing and looking towards, while on the service side, how we're going to do that, i.e., budgets, programming, analytics, resources, all these kinds of things.

To your question about initiatives, we're working on a broad range of things. Specific to CT, we are focusing on how the CT mission fits into an increasingly crowded field of priorities for Special Operations.

In other cases, it's the flip side of that. We are making the case that the SOF enterprise is not just the 'CT force.' It's key for us to balance the right allocation of not only what training and how we are the building our forces but also making sure that operationally we are deployed to the right places with the right proportion of forces.

CTC: Over the course of your career, you've worked on CT issues in a variety of different roles, including time at the National Counterterrorism Center, the National Security Council, and as director of the Pentagon's Defeat ISIS Task Force, which you helped to stand up. What are some of the key things that you learned from each of these CT-focused roles?

Maier: There are certain evergreen issues that I've taken away as I build my professional experience toolkit. One of those is risk and how risk is managed from several different perspectives. There's operational risk, of course: risk to mission, risk to force, and having a much better understanding of how our Special Operations enterprise goes about thinking through that. Again, not only at the tactical, but also on the operational level. Then there is also risk in terms of how much we invest in certain areas and partnerships.

From my NCTC time and especially at the National Security Council staff, understanding how that risk plays into the broader national security or policy risk is key. Things that might seem obvious to the CT professional to do can change once compared against a whole series of other things. It could be the public optics of doing something, working with a government, or simply not being too invested in certain areas that could reduce your decision space.

I think for many of your readers, understanding those differences as they relate to risk and accepting risk are a key part of the 'CT value

"The evolution of CT is a testament to what the U.S. government and in particular the Special Operations enterprise can do to evolve against the problem set."

chain.' We also have to consider what authorities we can operate under and if we are working alongside our allies and partners and what are their limits.

CTC: When you look back on where CT has been, how would you characterize its evolution and how would you describe where we are at the current moment?

Maier: I think the evolution of CT is a testament to what the U.S. government and in particular the Special Operations enterprise can do to evolve against the problem set. If you think back to what the world looked like in 2001 or 2002, and some of the decisions that were made to go 'big and loud' into areas like Iraq, Afghanistan, proved that 'big and loud' was not a particularly sustainable approach. More importantly, not sustainable with small SOF teams going it alone either. We've looked for hybrid ways from the military perspective to get after this problem.

One of the things that I think is a profound takeaway is the integration across the U.S. government and the CT community. I used to be surprised when I would step out of the CT role and see that other communities in our own U.S. government didn't have nearly the degree of integration or breadth [that] we have in the CT environment—by that, I mean working with law enforcement, the State Department, the intelligence community, and our allies and partners. This is something the CT community continues to do well and build upon.

Within DoD, especially in the SOF enterprise, we've proven how being 'joint' can be a force multiplier. In SO/LIC, we often talk about the idea of needing to maintain a degree of jointness at a very low level. It could be the O4-O5 level that's interchangeable parts between a Navy Special Warfare Operator or an Army or Marine Corps or even Air Force Special Operator being able to fill similar roles. This is a particularly profound degree of integration that we want to keep going.

Your question of where the CT problem set is now, I feel it's gone through a couple generations. We went through the al-Qa`ida generation, broadly in the 2010s, and then the ISIS generation over the last decade. Watching some of the changes in how the U.S. government approached these CT threats, they are admittedly not the same problem set. But we've learned much more in the ISIS problem set as a coalition, bringing everybody along.

We now have 86 countries in the Defeat -ISIS (D-ISIS) coalition, which doesn't get nearly enough attention, but we meet with them regularly. All 86 of those countries, and other organizations such as Interpol, get something out of their involvement. The coalition we have worldwide has become a foundation to build upon for so many other things.

I think this is the future, as we look at trying to do more with the same or more with less in the CT fight, finding ways to keep some of these sustainable elements going. A lot of that is looking to our allies and partners, looking to the U.S. government as the convener of those allies and partners to be the magic that makes the entire enterprise go smoothly and be productive. The classic 'sum greater than the individual parts.'

CTC: In a recent interview, you mentioned that you are the oldest of seven children. What impact has that part of your background had on how you fulfill your responsibilities here in this position, particularly in advocating for SOF within the Department?

Maier: I might have a different answer than my brothers, sisters, or my parents; they would probably say that I was the bossy one. But it's a good question because I think it taught me early on that building coalitions is important, and I've seen how important coalitions have been throughout my career, especially in the CT fight.

My father was a civilian for the Navy his whole career, which drew me and many of my siblings into public service. I think, especially in my formative years when CT was the 'fight,' it made sense to really lean in on the value of coalitions. I've built on that to understand, at least from the perspective of not being a military member of the SOF enterprise, but as a civilian, what makes the community tick. How the community is viewed by the outside and [how it] views itself can be very different. Does that all come from fighting over who gets what at the dinner table, I don't know. But these are things that have forced me to think more comprehensively at times than maybe I would if I had a different experience growing up.

CTC: Over the past several years, the U.S. counterterrorism community and the U.S. government in general have been trying to navigate how strategic competition and counterterrorism intersect or interplay with one another so that the U.S. counterterrorism enterprise can be calibrated to open up space for the U.S. government to focus more intently on the pacing challenges from countries like China. Your office sits at the policy and practical intersection of those issues and questions. What does that response and adaptation look like from your vantage point, and are there any examples that you can share that speak to those?

Maier: We're at a point of both continuity and change. The continuity pieces of CT are not going away, and are in fact certainly implied, if not explicit, when you look at the some of the goals in the National Defense Strategy: preventing strategic distraction or making CT central to our national security thinking once again.

We need to have sustainable CT operations that prevent terrorists' actions, principally al-Qa`ida and ISIS, to ensure we are not distracted by what we view as the longer-term strategic priorities, such as peer adversaries.

As I mentioned earlier, as the rest of the Department and other parts of the U.S. government are doing less CT, [this] means that those who are doing it have to do it better and, in many respects, do it more proportionally to the rest of the national security enterprise. This is why SOF is looked to as the lead for the CT fight in the Department. The big change is the National Defense Strategy asks us to do integrated deterrence and campaigning. From a SO/LIC

Christopher Maier

and SOF enterprise perspective, it is shaping activities prior to conflict to prevent a full-blown, large-scale combat situation.

But if we do have to go into conflict, then you want the best odds for your side as possible. For SOF, that relies on our ability to build key ally and partner relationships. That's making sure we have the right people in the right place who are making the right decisions for senior leaders. SOF has been fighting [the] CT [fight] for a long time, as shown in a lot of movies about SOF's CT fight; we've been doing the integrated deterrence piece and campaigning for years and years.

If you look back to the example of some of the seeds planted in Ukraine, we're now reaping the benefits of 2014 training and engagement opportunities. Those are the core issues that we're working through and how we consider the SOF value proposition in the places that don't get a lot of attention. As the entire Department, maybe even the U.S. government, tries to figure out what it means to grapple with an emergent China and certainly a Russia that's hard to predict, but it's also about figuring out where SOF fits.

Everybody knows the Special Operations piece, but the low-intensity conflict piece is a bit of an antiquated term. But it refers to many of the same things we're talking about such as shaping the information environment and leveraging things like irregular warfare as a concept.

We're trying to work across the Department to expand this idea beyond just a SOF value proposition, and how the Department thinks in asymmetric ways. There is value in being able to operate in ways that the military may not be the primary lead but can create dilemmas for our adversaries and decision space for our senior leaders.

CTC: You mentioned integrated deterrence. When you think about integrated deterrence and how CT can be a component of it, what does that look like to you? How would you describe that? What role does counterterrorism play as a form of or part of deterrence?

Maier: Take the term first—integrated deterrence. There are lots of people smarter than me that have spent a lot of time defining this term, but I will break it into its core parts. 'Integrated:' when that first came out, it was like, 'We're golden. SOF knows how to do integrated.' 'Deterrence:' causes somebody to do something that they otherwise wouldn't want to do or don't see as in their interest to do.

There are many elements in CT that are very applicable. People don't talk about it as much, but the degree of operational prowess that the United States has because we've been doing difficult things in an operational sense for 20 years, is in and of itself a deterrent against adversaries who may have not gone to war for generations.

We have the ability to do very exquisite things from great distances in a very precise and risk-managed way. That is something lots of people study but something not many militaries in the world can execute. That in and of itself is a deterrent.

Then there are the pieces more commonly talked about: having that placement and access, having the ability to operate in a number of places in proximity to adversaries on their periphery is something that they have to spend time thinking and worrying about.

Our allies and partners are also a critical piece to the SOF enterprise. In fact, in many cases, the value proposition of things like 'by, with, and through' is predicated on having allies and partners increase their capability and coexisting with them. There's just a depth there of partnership that doesn't exist in the same way in some other warfighting disciplines and certainly not for adversaries who are hard pressed to find one ally or partner. It's not a surprise that Russia and China are having to become closer with one another as partners, because there isn't anybody else that's wants to be on their side of the table.

These are all things that are huge advantages for us, and whether we're looking at it through the narrower SOF perspective or broader as a U.S. government, we have several advantages that have been fundamentally built over the last 20 years of the CT fight. That's something we continue to lean into, and we should see those as mutually reinforcing, not in competition with one another.

CTC: What advice would you offer for how our community can think about—particularly in the counterterrorism realm—how our efforts to pursue and navigate these complex set of priorities is being effective? How would you think about that?

Maier: The measure of effectiveness is challenging for a number of reasons. One, the 'absence of' is often our measure, and that's a particularly concerning measure. You're trying to ensure something doesn't happen. Let's take China and Taiwan, for example. We're very focused on there not being some sort of cross-straits military aggression towards Taiwan, and that means every day—when there is no aggression, it is a good day for us. Similarly, we would have said, 'Hey, there hasn't been any terrorist attacks.' But that is the very basic, most simplistic way of thinking about it.

We need to then pull on those threads and figure out—and this is where our intelligence community is absolutely our number-one partner—how we think the capabilities of groups or countries are

going and where do we see that intent going?

Capabilities are often much easier to track than intent. Where the CT fight becomes a little bit harder to use as a model for the nation-states' struggle or competition is we always assume that the intent was there for most of these individual terrorist groups, networks, cells, whatever groups, and it was just the capability that was going to determine the level or type of threat. There was very little to deter them, and this is what they were ideologically focused on.

Nation-states, especially in the case of adversaries like Russia and China, have a lot of other things they're weighing, and that makes it that much more challenging to measure. We probably need to be humble from the DoD perspective that we're not the lead lever, especially in nation-state competition, the same way we were in the in the CT fight.

The classic 'have hammer, see nails'—if the military instrument is how we're thinking about this—we need to be very cautious about how we fit into that, but at the same time not necessarily always assume that we're in the supporting role. There may be times that the military instrument—especially short of war, back to the SOF value proposition—can be particularly compelling in creating a value chain.

We talk here a lot about kill chains, but if we think of it through a more interagency perspective, there may be elements where SOF can be a key node in a network that helps to build access for collection in support of the intelligence community and perhaps using some non-lethal effect in a different way than maybe we thought about in the past.

So, there's the measure of 'are you actually having impact on the enemy' and increasingly, I think that's going to be in the cognitive space. But then as we look at our own way of projecting capabilities and ability to achieve the effect we want as precisely and risk informed as possible, [it] is something the DoD is going to have to figure out. Where do we fit into an all-of-USG or all-of-allies-and-partners approach? That's something that is very challenging to do because it's going to be very fact-specific, too.

CTC: You've talked about partnerships quite a bit. If we could hone in on the future of CT partnerships specifically, how would you describe the appetite for that partnership? How do you ensure that the future of those partnerships is strong and that they continue to evolve in the way we want, and our partners want as well?

Maier: If these partnerships aren't nurtured, they will start to fade away. Not because some of our closest partners won't want to work with us, but because they will begin to invest in other things. At the end of the day, they'll be watching us and will be making their own national decisions.

I'll go back to the heyday of when we were doing combined operations with Five Eyes partners, NATO or other capable, global partners. We're doing less of that now, so that puts more onus on finding ways to continue to stress-test our own ability to work together, and it also means investing in the same types of interoperable capabilities, too.

As we've seen in places like Ukraine and still in the CENTCOM area of responsibility, if we can still work with other partners, we're going to be able to respond in a credible way much more quickly. But if some of that intense cooperation starts to fade—here, I'm talking about not only TTPs in the human dimension of different operational elements being able to work together, but also having complementary technology, if not the same technology—it's going to be important.

The CT space, though, is still one where we do things more operationally than we do in some of the other areas that might be priorities. We need to continue to look for opportunities to bring our allies and partners into that, even if the problem set reduces.

For example, in the mid-2010s in Iraq and Syria, we had a lot of partners who had deployed forces that were supporting different parts of the D-ISIS mission. There is now a much smaller force footprint, so that means fewer opportunities where we're working together. Recognizing that is probably a sign of success, but at the same time, it presents some challenges for how we retain a credible combined force. We're going to need to continue to lean into areas where we can work together, more jointly, such as exercises and experimentation, recognizing that they might seem more artificial or more contrived. That's the reality we are facing.

There's a lot of emphasis around the Department toward broadening how we engage in our partnership building. There are a lot of other capable, credible partners that we're going to need especially if we're looking at the Russia or China scenario.

CTC: Technologies like artificial intelligence, machine learning, and data science-driven approaches have already begun to revolutionize and in some cases have revolutionized how DoD and SOCOM approach data, what can be done with data, and the speed of those decisions. Can you provide a high-level view of how that world's evolving? How can the Special Operations community, as it moves towards that AI/machine learning-driven future, maintain focus on other core principles in addition to the speed of Special Operations success, including simplicity, security, repetition, surprise, and purpose, as Admiral McRaven outlined them several decades ago.[1]

Maier: Obviously, technology is extraordinarily important, and it's going to be fundamental to how we fight or prevent wars in the future. From a SOF perspective, we need to be conscious of continuing with the term of art 'SOF-peculiar.' What is the SOF value proposition of some of [the] things you listed: AI, man-machine teaming, call it decision-support capabilities. Everybody's trying to develop these, and there are several initiatives here in the Department to try to do it as jointly as possible, even as the services create their own specific ones for a maritime environment, an air- or land-based one.

We need to be conscious of the fact [that] we have a much smaller budget and a lot less ability to generate, even with some of our unique acquisition authorities in the SOF enterprise, those things that are adding value on top of what the rest of the Department is doing for those SOF-type missions.

There are some elements of the SOF enterprise that are important to keep in mind. For example, many of the information forces in the Department fall in the SOF enterprise. We need to be very focused on building capabilities that can affect the cognitive space of not only our adversaries, but also in some respects the broader set of people who are looking at what we're doing. By that, I mean our allies and partners, and our own nation. I'm not at all suggesting that from a DoD perspective, we should be influencing the information environment, but the reality is that we need to be

able to play defense against adversaries who are much more inclined to take a less principled approach to how they use information—truth versus fiction—and recognize that that's ubiquitous. We need to be able to harness some of those aspects of the information space from a SOF perspective to make that one of our warfighting competencies.

Some of the other things that you're talking about need to be viewed in the context of how SOF can operate: probably still in austere environments far away from where large military formations are going to be. We're going to need forces that can do a lot of things simultaneously.

By that I mean, the colloquial is, the Swiss Army Knife. You might be one day part of a SOF unit doing training or building partner capacity for a unit, and, if something happens in a crisis situation, you have to call in fires, use cyber capabilities or maybe it's the placement and access that will contribute more to bringing space or electronic warfare tools to bear. It's going to have to be done in a small enough unit so as not to attract attention the same way a large formation would. Looking at technology in the context of the actual operational use and value is going to be important, and something this community has long done well.

We often talk about the overhead intelligence collection platform. Increasingly, we're seeing opportunities to use large amounts of data for more horizontal information situational awareness. Obviously, the intelligence community is very focused on these uses as well. I think our value proposition is how are those operationally useful, not just for the purposes of collecting intelligence and analysis, but for things that have to be collected, quickly analyzed, and put into practice. Especially if you're talking about a small entity with probably austere challenges and likely far away from any traditional infrastructure. This is a lot of where I think we're already going, but I think we're going to need to continue to lean in on that. Again, I go back to how we started the question, which is looking for those unique value propositions that only SOF can bring and really leaning in on the technology assistance to that.

CTC: As you know well, as the United States is evolving and adapting its approach and embracing technology and experimenting and innovating with technology, its adversaries—particularly on the non-state actor side and the proxy side—are always trying to do the same thing. In January 2021, the DoD released its counter small unmanned aircraft systems strategy and identified SOCOM as the responsible party for developing and implementing the left-of or prior-to launch component of that strategy.[2] Can you provide an overview or an example or two that illustrates how the ASD SO/LIC team and SOCOM have been dealing with the challenges that dual-use technologies present, which sits at this heart of the counter-small UAS problem set?

Maier: First, let's talk about unmanned systems. We have long used unmanned systems and those were big; like most technology evolution, they are now getting smaller and smaller. It's been a comparative advantage for us operationally and strategically. I would say the rest of the world is starting to catch up at a much faster pace, as these things tend to go. Not only are we in a situation where the dual-use aspects of this increasingly have a military element to them, but the barriers to entry have significantly declined. We must spend time not only thinking about how we project, but also how we would defend against. I think the current Israel-Gaza crisis demonstrates just how much adversaries—in this case, Iran and Iranian-aligned militia groups—have been able to quickly move up that technology sophistication. Ukraine is maybe the poster child of the unmanned fight.

"We need to be able to play defense against adversaries who are much more inclined to take a less principled approach to how they use information—truth versus fiction—and recognize that that's ubiquitous. We need to be able to harness some of those aspects of the information space from a SOF perspective to make that one of our warfighting competencies."

From SO/LIC, working with SOCOM, figuring out ways to get at this problem set before you have to interdict it on the battlefield is really important. One of the things that SO/LIC brings to the table is being a Washington-based interagency manager, we have several interagency relationships and a lot of experience in working with them. The way we're thinking about this particular issue of counter-small UAS is SOCOM working through a lot of the operational initiatives and different concepts. Additionally, SO/LIC works with the intelligence community and other partners that are a little less traditional, like Departments of Commerce and Treasury, who have the ability to sanction countries that prevents some of these things from going to other places. We've done some of this over the years in the CT space, but usually not as directly against a unitary problem set, and I think that's a bit of a blueprint for a lot of other areas.

Now, let's talk about AI. AI certainly is going to be something that we will find is ubiquitous to increasing lethality of foreign militaries as much as it will be for us. Finding ways to think of how these components, how these different approaches often come from outside conflict areas, often from areas that are 'first world'—if we can use that term—and figuring out how some of those components don't flow in a way that they can be quickly used to create battlefield effects for our adversaries.

When we started out doing CT in the first few years after 9/11, we didn't talk much about 'agnostic finishes.' Now we spend a lot of time and invested a lot of resources in helping law enforcement take terrorists off the street, so to speak, or finding ways to interdict financial transactions that aren't a military effort in the first order. But if we have information that can then be systematically provided to these other elements of the U.S. government or allies and partners, we have found a way to do that.

I think we're going to need to have a similar approach to technologies that we want the good to get through, but not the bad. How we create that filter across much different enterprises, systems, and economies is going to be something we're going to have to think about.

CTC: You mentioned technology being a component of the

ongoing conflict in Israel, Gaza, in Hamas' attack, and the dynamics that have been playing out with other players after that incident as well as with the conflict in Ukraine. Is there anything else when you look at those two conflicts that you think is important to take away as key aspects to think about when it comes to counterterrorism?

Maier: The most obvious one in Israel-Gaza is the idea that this terrorist group isn't the same as we saw with ISIS and al-Qa`ida. To mean, one that has terrorist elements but also governs and does a lot of other things, and one that we probably weren't as focused on because it was an Israel-Gaza problem. I think it underscores again, what feels like has been the case in the last couple of years anyway, a lot of surprising, destabilizing global events.

In the case of Russia-Ukraine and Israel-Gaza, these are areas that have flared up in the past, and we probably didn't think that they were going to flare up quite the same way that they have. So, we're trying to look to what we see as the future strategic challenge in the Indo-Pacific and an ascendant China that probably has a lot of designs on dismantling the world order we've come to depend on. I think it's being able to do all those things and figure it out from a SOF perspective.

There's a continuity aspect of being able to provide our allies and partners those capabilities that we've developed, and have learned in many respects, how best to transfer them and continue to do that work with our allies and partners in the lead as we manage crisis responses that always comes up in each one of these incidents. Things like where U.S. personnel are located, whether those official or unofficial U.S. personnel are being prepared to provide what I think is our sacred responsibility to keep them safe in a SOF-lead mission.

And then the other piece of this is recognizing we must do all that, but at the same time, we've got to create the advantage for the United States—that prior-to-conflict piece. It's really being able to do a lot of things with a budget that isn't getting bigger, even though we have a massive budget in the Department of Defense. The challenges seem like they're getting broader, and they're a lot more expensive when you're talking about the kind of technology we've already talked about, and being able to, in some cases, provide large outlays of equipment and munitions to allies and partners as well.

From the SO/LIC perspective, SOF is involved in all of these. We're at that intersection between non-state and state actors all the time, and it's those things we've learned, especially in the CT fight against non-state actors, that translate to supporting a state in some cases, resisting the aggression of another state. While at the same time, we cannot lose sight of the fact that we need to continue to develop our capabilities against non-state actors because they seem to be of all different ilks, and they continue to cause significant national security challenges for us.

CTC: As our over-the-horizon strategy reallocates limited resources to accommodate changing priorities, you look at something like the al-Zawahiri strike, which is an exquisite example of it, but the further we get from boots on the ground, the harder it is to do some of these things. Do policymakers still expect the same results, and how do we mitigate some of that?

Maier: I feel like policymakers—and it's easy to talk about them in a general sense—still expect the same results, and I think that puts an onus on how the CT fight has had to change, and for good reasons. I'm not sure in all instances the proximity necessarily created a better outcome in some of our large combat points or even smaller ones in Iraq and Afghanistan.

I think there's a balance between being able to be proximate enough to be able to mitigate some of these threats and being able to do that with our partners and allies. In many cases, we're talking about partners who are not that capable, often dealing in a semi-permissive, if not permissive environment, for these non-state actors or CT problems because there's fundamentally not a lot of governance in these places.

How we strike that balance is going to be important. It's a fundamental feature of many of our policy debates and how much you need to invest to get the effect you want, but also how do you avoid overinvesting or underinvesting while at the same time needing to put this in the broader context of other strategic objectives we're trying to achieve?

I personally hate the term 'over the horizon.' We've used it ourselves in the Department, but in CT, we've always been doing it to some degree 'over the horizon' because not all the capabilities were right there. As we're increasingly challenged by adversaries for our own placement and access, even in places like Iraq and Syria, we're going to have to rely on some of those technology solutions, but also understanding what are the necessary components of a partnered strategy and what can partners do for themselves or with different tools, perhaps with less than we've been able to provide in the past? That's always taken in the context of what the actual threat is to the United States as well.

CTC: What terror threats concern you the most as we look towards the future?

Maier: The one that continues to concern me is the one that we're not seeing. We've often thought of terrorism in a very specific and directed way, such as the 9/11 attack, that is fully cooked up overseas and brought to the United States. Then, there's one that's more facilitated that got some overseas support, but they also had local folks doing it.

And then there's the inspired one that increasingly has been a function of ISIS and al-Qa`ida in large portion because they can't do one and two; those are hard to track because all it takes is an individual to make a decision to do something.

I am particularly concerned about those that probably have the hallmarks of a small group of radicalized individuals that might be well below the radar screen of what we're looking at, [but] that can harm Americans. To be frank, what is not clear to me at this point is how much our resilience as a nation over the last 20 years has evolved. Does an attack, especially if it is particularly damaging to Americans, cause us as a country to change our overall national security strategic approach? Or is it going to be something that we look at and look to mitigate the reasons for it, but keep our focus on the strategic objectives? I think we spend a lot of time playing that out in systematic ways and in some cases, informal ways to figure out what are we missing here.

Unfortunately, in this line of work you're always looking for what you might have missed, because it's what you missed—an attack that was unanticipated—that will force us to take our eye off some of these strategic challenges. CTC

Citations

1 William H. McRaven, *Spec Ops – Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press, 1996).

2 "Counter-Small Unmanned Aircraft Systems Strategy," U.S. Department of Defense, January 7, 2021.