A View from the CT Foxhole: Charlie Winter, Co-Founder, ExTrac AI

By Paul Cruickshank

Dr. Charlie Winter is Co-Founder and Chief Research Officer of ExTrac AI, an intelligence platform that tracks conflict and information activities to identify, map, and forecast geopolitical risk. Before ExTrac, he worked in a range of academic positions in the United States and United Kingdom, researching what drives and perpetuates violent extremism in both online and offline spaces.

His academic research was supported by the U.S. Department of Defense, the Global Internet Forum for Counter-Terrorism (GIFCT), Facebook, the UK Home Office, and the U.S. Department for Homeland Security, among others. He is an Associate of the IWM, an Associate Fellow at the International Centre for Counter Terrorism in The Hague, and a member of the RESOLVE Network's Advisory Board. He has published two books, The ISIS Reader and The Terrorist Image.

CTC: Let's start with your professional journey and how you went from a mostly academic research focus to founding ExTrac. Can you describe that journey?

Winter: Across most of the 2010s, I spent a lot of my time lurking in parts of the internet that Islamic State supporters were also hanging out [in], and my academic research essentially pivoted around the data that I could collect from those spaces and then analyze with a view to understanding what made the Islamic State—and to a degree still makes the Islamic State—tick. So, I spent a lot of time studying its propaganda in particular, and my PhD research focused specifically on the photo reports that it used to publish by the dozen back in 2015, 2016, and 2017.

It was really through that work that I got looped in with the practitioner community, working as an academic advisor to ongoing programs that were being implemented in the context of various stakeholders in the counterterrorism domain. And the work that I was doing in that capacity was essentially the same as what I was doing as an academic, but with the timeline truncated very significantly. Because while it's interesting to see what made the Islamic State tick in 2015, when you're a few years on, it's not necessarily useful from a practical or operational perspective. I found that [with] the work that I was doing, the timeline would get shorter and the analysis that I was being asked to provide would be not 'what are things looking like over the course of the last few years?' but 'what are things looking like over the course of the last few months, if not weeks, if not days?'

The question I increasingly found myself asking was how can you do something that's actually useful with this stuff [on a timeline] that matters and also improve on the technology side of things? For most of the 2010s, I was working in Excel, building out unwieldy spreadsheets and creating ugly visualizations of the data that would end up in academic research articles. I ended up teaming up with an AI guy and an entrepreneur, and that's when it all really started to come together. Fast forward a few years, and we have quite a significant team that really joins up domain and technology expertise. What I am now able to do, and what we're able to do at ExTrac, is essentially take that data and analyze it, visualize it, mine it for insights at the time that it is most relevant—so as close to real time as possible, with as little latency as possible—so it can provide meaningful insight to practitioners when it matters and doesn't just remain something that's interesting to look at in retrospect.

CTC: What services does ExTrac provide?

Winter: We are a geopolitical intelligence platform that helps people make decisions faster, and from a base of real evidence. Whether they are in defense, tech, development, finance, or something else, it's about enabling decision-makers to get ahead of the threat, or indeed the opportunity. Our USP pivots around accessing, ingesting, and processing high-relevance publicly available information and data from hard-to-reach parts of the internet that reflects the online and offline activities and psychological operations of various non-state and state threat actors. And through our platform, which is both a web and mobile app, we provide both access to that data and the ability to generate insight from it rapidly—and we do that using a range of different kinds of automation, machine learning, artificial intelligence. But essentially, it's the data itself that we're providing to our users and then also the ability to extract usable information from it at pace. Everything is auditable. Everything is very visual. And we think very carefully about what data goes into the platform in order to make sure that for our users, when they access it, they are looking at stuff which is directly and invariably relevant to the use case that they have.

One point to draw out which is really important is that there's a lot of data that we don't go after. We actively and willfully are not interested in user data. We don't want to know who's saying what; we just want to know what they're saying or what kind of content is being shared, what kind of platforms are being used to engage in terrorism financing or what kind of documents—instructional materials—are being passed around, that kind of thing. It's the content and the attitude, the narratives, the manifestos, the ideas and how they relate to activity in the physical world that are most interesting to us. They provide layered cognitive and kinetic insight into what adversarial actors are getting up to on a day-to-day basis and also how their activities—their strategies, their tactics, their targeting parameters—adapt to or are forced into adapting to counterterrorism operations or other efforts to interdict what they're doing.

CTC: How do you identify helpful and relevant sources?

Winter: We are split between engineers and subject matter

experts, broadly speaking, in the team. The engineers deal with the front- and backend of what we do—the models that we use, broad functionality, and how everything comes together at the user end. The analysts we have are deep subject matter experts in a range of different things. There's jihadism, all of its various manifestations and guises. But we also have specialists in violent neo-Nazism and accelerationism, and same for the key players in most of the other places where there are live conflicts. Essentially, what we do is hardwire their expertise into what is available within ExTrac.

With my ISIS 'nerd' hat on, I know from my past and ongoing research where people in groups like ISKP [Islamic State Khorasan] or [Islamic State] Somalia province are getting together, sharing content, networking, and so on—and much of this stuff is happening in spaces that are technically publicly available is going on. We work on that same basis with the other analysts that sit within our team. Through their research, through the time that they spend and have spent absorbing and internalizing the dynamics that characterize how these actors are communicating with each other—we *use* that knowledge, that know-how to determine and delineate what sources are relevant and, as you say, helpful. And we keep it up to date, day-in, day-out, so when one platform or community goes out of fashion or is rendered inoperable, we—and our users—can follow the ecosystem's migration into the next one.

The bottom line is, when we bring data into ExTrac, we only bring data that is coming from spaces that we *know* to be relevant to the actors that our users and we are interested in understanding. And it's all predicated on the idea that there's loads of information available to us now: publicly available information, commercially available information, there's a flood of it. But unless you curate the sources that you're interested in, you end up with just a lot of noise. So, what we do is curate by source rather than by data point, and we provide a secure service which allows for high-signal, low-noise information to be streaming into the platform and made available to our users around the clock.

CTC: So, to sum it up, the 'nerds' focus the laser beam, and then you get all this data. How do you then parse it for insights that can be helpful to practitioners?

Winter: The data goes through a whole pipeline of cleaning, enriching, and tagging to organize it and make it readily searchable—that's where the AI first comes in. Once it's been ingested into our databases, we have a number of models and search functionality that helps our users find insight around aspects such as targeting trends and messaging. Core to the system is Co-Analyst, which is the agentic large language model integration we have that sits at the center of everything.

Essentially, the platform in which this all comes together works by enabling users to set up different dashboards that correspond to the different geographies, different actors, different use cases that they might have. And within each of those dashboards, you can set up communication streams or event streams along with associated mapping or analytics layers like topic modelling, salience analysis, or network graphs. We have an event detection model that sifts through all of the data points that we're ingesting—whatever the platforms we're ingesting it from—and looks for references to kinetic or conflict-adjacent incidents. This means you can see what SIGACTS are being reported by the actors in question—their members, their rank-level members, as well as in official propaganda reporting, too. We then triangulate that with reporting we're ingesting from unaffiliated sources and use machine learning to identify the delta between the two. That all gets mapped and chrono-located as well so you can see, and be alerted in real time to, what the actors in question are saying at the official level, what their supporters and rank-level members are saying to each other about the world around them, and what the rest of world thinks, too—and then visualize it all through maps and time series graphs.

Charlie Winter

You can monitor, for example, how frequently threat actors are discussing shipping activity in specific locations, assess the nature of that conversation, identify indicators of imminent threats to commercial or naval vessels, and track chatter about the courses of action that these actors are most likely to pursue.

The key thing is that we are moving analysts away from having to scroll through a lot of data to try to figure out what the consensus view is about something within the ecosystem in which they're interested—because of how the artificial intelligence and specifically Co-Analyst enables the data to be parsed, analysts can use our LLM, which understands 245 languages, to monitor the strategic, tactical, operational, and cognitive environment at pace and in a manner that more accurately reflects what's happening at the coalface. Through our system, analysts are able to effectively process hundreds, thousands, tens of thousands, hundreds of thousands of data points in a few seconds, rather than having to spend—as I used to do as an academic—days, weeks, or months coding an Excel spreadsheet to generate visualizations that would then be reflective of the interesting but old data behind them.

Everything we do is about using technology in a really, really constrained way and recognizing its limitations, but also recognizing the limitations that *analysts* have and the unending and invariable issue around time, resource, ability to juggle multiple intelligence requirements at any one point in time. We essentially have built our system to let machines do what they do best and let human analysts do what they do best, and enable the analysts to spend a lot more

"We essentially have built our system to let machines do what they do best and let human analysts do what they do best, and enable the analysts to spend a lot more time performing the highest-value tasks in the intelligence cycle."

time performing the highest-value tasks in the intelligence cycle—figuring out the 'so what,' identifying implications, putting together assessments based on data that is both more expansive than what they'd be able to do if it was them working manually through the same data points—but also enabling them to use and apply quantitative methods in a way that doesn't feel like quantitative methods to visualize and identify patterns and anomalies without needing to come to the table with a bunch of data science expertise.

CTC: So, you have, in a way, the best of both worlds because you've got people like you and other analysts who have, in your phraseology, 'lurked around' this stuff, scrolled through this stuff. You have a feel for this stuff as an analyst, and that has obviously contributed to the way that you've been able to focus the laser beam and the inputs you've put in on the AI. Is there a danger that as more and more analysts move to the high-level stuff, as you put it, that we lose something from that experience of actually having to go through it oneself. Is there a danger of missing stuff?

Winter: It's a really good question. The fundamental thing that we are doing at ExTrac is making more, better, more relevant open-source data available to our users than they'd be able to access on the systems they have in the environments in which they're working. We are enabling them to have much closer access and more engagement with threat actor ecosystems than they would otherwise have. All of the data that comes into the system, we identify and tag the sources that we ingest it from, and there is a total air gap between what happens in ExTrac and what happens in the outside world. So, you have people who normally would not be able to jump into the middle of a terrorist chatroom being operated from denied territory, for example, who now are able to engage with that data, see it in the wild—as it were—but then also analyze it in a way which is safe and much more ambitious than would have been possible before.

The other thing is the way that the technology enables us to work across languages. This means that you don't need to be Arabic language-enabled or a Somali speaker to be able to dig really deeply into the information that we're looking at. If anything, we're providing better access, more access, deeper reach into these phenomena than was possible before we set up shop.

As a founder of ExTrac, obviously I'm doing lots of stuff that isn't analysis, but fundamentally, I'm still an analyst at heart. I still spend a huge amount of my time in the system—probably too much time—using the system to dig into things and explore what's in the realm of the possible just because I find it interesting to do so. And in contexts in which I had no prior expertise or knowledge of before, I can go far; I can get deep into Swahili- or Tajik-language terrorist communications in a way that would never have been possible before.

Crucially, our offering isn't just about being able to see the data and get a feel for the data. It's also to enable and provide that quantitative element that I spoke about before: being able to actually visualize how salient a particular thing is or how far a piece of content has spread or how much a conversation about an imminent threat of violence might be to an embassy, say—being able to say and situate that particular data point within longitudinal data, to see that this thing is actually gathering a lot more momentum than at other points in the last 12 months where similar conversations have been had. That kind of thing just enables you to have a much better grasp of what's going on in the mind of the adversary than was possible before.

CTC: Are you able to get more specific in terms of, over the last several years, where the biggest value added has been in looking at certain trends that you were able to help clients identify?

Winter: As well as identifying things that no one knows are about to happen, a key part of what we do is corroborating intelligence to make it easier to pass between organizations or allies for actioning. We do that based on stuff which is in open source or hard-to-reach publicly available sources. A good example of this from a while back was when the Taliban took over Kabul in the summer of 2021. Our system identified for us that there was, at that time, a meaningful change in the way that ISKP both at an organizational and supporter level was communicating—to such a degree that, in some previously busy online spaces, there was a total blackout. This wasn't down to the sources themselves going dark; it was down to an organizational push on ISKP's part, and it was 11 days before the attack on Kabul International Airport took place. The system alerted us to this change—which, it turned out, the intelligence community was also tracking but not yet talking about—so we could tell our customers that something was up, that something big was looking like it was going to happen. We were observing an ISKP that had, up until that point, been in a period of ascendancy suddenly shutting up shop. Crucially, this change wasn't noticeable on a day-to-day basis—as in, if you're looking at individual data on individual days—but when you take a step back and look at trends up to that point, it was clear that the operational environment was going to change in quite a profound manner.

In short, it was a change in both the information and kinetic posture of ISKP that was totally inconsistent with the shape of the previous 12 months' worth of activity. That pause was something that directly preceded the attack on Kabul International Airport, but also in the days that followed it, the launching of an Afghanistan-wide campaign against the Taliban when it was in its first few weeks of ruling Afghanistan. And it's that dynamic, that change in both operational and information posture, that we're interested in furnishing our users with from an indicators and warnings perspective.

CTC: So, it's an indicator for a potential beginning of either a very significant attack or series of attacks, and you were able to identify that in real time. But, of course, knowing that an attack campaign may be in the works is different from knowing where

and when a particular attack is going to happen.

Winter: It definitely is. So that ISKP experience—early on in ExTrac's journey—was one of a few points at which we understood that there are indicators in communications data for stuff that will impact the offline environment, potentially very significantly. So, building on it, we trained deep learning models to identify similar lapses or anomalies or surges that were statistically significant. These have enabled our users in the years since to add to their assessment of both information and kinetic threats in relation to the positions, people, and assets that matter to them ahead of attempted or indeed successfully deployed incidents or campaigns taking place.

We also pick up and alert for indicators that are more blatant. When you are operating in the context of non-state actors, and specifically terrorist actors, their supporters actively share attack-planning materials and flag individual-level intent to engage in terrorist behaviors—whether that's sending money to different parts of the global network, for example, or, on the more operational side, actively planning and discussing targeting of specific people or places with others in the ecosystem. In the terrorism context, these are the things that we're able to essentially listen in on.

We also are able to identify what's coming down the line in very dynamic, very live situations. When, for example, there's a conflagration somewhere involving supporters of a particular threat actor, we can help our users understand what those supporters are gearing up to do. For example, when threat actors have in the past launched PSYOP campaigns online or raided diplomatic complexes offline, essentially looking to besiege and ultimately overrun embassy facilities, we've been able to pair up what's happening on their side—what they're saying, what their leaders are telling them to do—with our users, getting them, in an air-gapped environment, into the hard-to-reach but ultimately public chatrooms and channels that were being used to orchestrate these activities in the first place. They could see what these actors were saying about potential courses of action and factor that into the decision points to which they ultimately came, whether we're talking about information operations or force protection. Essentially, we can make our users a fly on the threat actor's wall, get them inside or close to the adversary ops room to enable them to listen in on conversations—happening in spaces that are hard to find and get to but publicly available—that are directly operationally relevant to decisions that they have to make without going near a secure system and put up with all the associated frictions.

CTC: When it comes to Yemen and the Houthis, talk about how your platform has been helpful.

Winter: In the context of Yemen, for the last few years, we've been doing a lot of work on the conflict there—capturing both what's happening at an official level and also, crucially, at a rank level, as well as what the general populace is making of things. So there are various things that one can derive from that data, both in relation to the force posture and intent of threat actors but also how those same threat actors are managing the domestic political challenges they face as a response to external pressures. Our system essentially enables you to identify the degree of threat and likelihood of that threat being acted upon in relation to specific targeting efforts or broader campaigns like the maritime blockade. With each stage of escalation, we've been able to determine both whether and when it was going to come to pass long before it happened and also determine that the threats were highly likely to be credible rather than just bluster.

This data essentially enables you to get deep into the mindset of these actors. We're able to track how—almost from a battle damage assessment perspective—the extent to which deterrence is occurring, or not as the case may be, as well as the extent to which deterrence *could* occur in response to the use of military force. So when thinking about the way these actors conceptualize their standing and strategies, we're able to provide insight that otherwise would be difficult to get to, about what impact (or lack of impact) a given campaign is having on morale, on intent, on decision points about continuing or not the activities that they're engaging in.

CTC: When it comes to other elements of the Tehran-aligned threat network including Hezbollah and the militia groups in Iraq, talk through how you've been able to provide insights in that space? Syria obviously as well until relatively recently.

Winter: We have done and continue to do loads of work on Syria. It was, from an analytical perspective, fascinating to observe the tectonic shifts that were happening in December when the Assad regime was on the cusp of falling. Right at the time that the regime was disintegrating, we were able to see that the Iranian position was not going to be one of intervention, again before it became clear that that was case. We were able to see this by identifying changes in the way that key players were referring to Hay'at Tahrir al-Sham as it was then. Essentially, just before Assad left Syria, they stopped referring to HTS as '*takfiris*' and instead started referring to them as 'rebels.' That softening of the stance at the official level, and also among sources associated directly with the broader bloc, was a very good indicator that the Iranians were not going to be shoring up the regime—let alone others in the network.

Similarly, in the context of Lebanon's political landscape—another area in which we've done a huge amount of work in recent years—we've been able to track fragmentation within key factions at its earliest stages, as well as changes in sentiment across the broader environment. Through the mechanisms afforded to us by artificial intelligence, we've been able to identify anomalies and new trajectories of engagement when they are still nascent, encompassing both factions traditionally supportive of the status quo and those historically opposed to it, as well as actors occupying the middle ground. We could also identify how Israeli military pressure was impacting and affecting change from the outset of the campaign last September, not just from a material or leadership perspective, but from a fundamentally strategic standpoint, altering how key groups viewed their roles within Lebanese politics and the broader region, including their ties with Iran.

Right now, we're using these same tools to gauge how steady the current ceasefire is, going beyond official rhetoric from the guys at the top to track how rank-and-file thinking has evolved, identifying trigger points and new red-lines for potential re-escalation.

CTC: Let's pivot to sub-Saharan Africa and West Africa because you do a lot of work there as well. And obviously, it's an area where when it comes to al-Qa`ida- and Islamic State-aligned groups, there's a huge amount of concern. Talk about West Africa.

"ISIS, which has very deep foundations in Syria, is not flexing its muscles there yet. I worry that it is more a question of *when* rather than *if*."

Winter: West Africa is the *pièce de résistance* of ISIS these days in terms of the space about which it's happiest and most enthusiastic to publicize its activities in. Obviously, that's due to a lot of different reasons. It doesn't necessarily mean it's technically strongest there; it just means that the organization has determined that it is less operationally risky for it to highlight the activities of ISWAP [Islamic State West Africa Province] and ISGS [Islamic State in the Greater Sahara] in that part of the world than it is to highlight them in Afghanistan or Syria or Iraq.

When you bring time series communications data or SIGACT data to bear in that context, [it] enables you to see clear ebbs and flows in the strategic calculus of the likes of ISWAP and ISGS—and the same, incidentally, can be said in the context of groups like JNIM. It allows you to identify different target sets that are likely to be focused on and, through that, the degree of threat faced by, for example, the development and humanitarian organizations that operate in spaces co-located with ISWAP and ISGS. Again, there is an enormous amount of utility in being able to see a given data point—whether it's a communication or an act of violence—in the context of everything that's come before it, to see the extent to which it is part of an ongoing strategic trend that's been around for months, if not years, or if a particular attack in a particular part of Borno state, for example, indicates a change in posture, a change in strategy, or that something new could be underway.

So again, based on that kind of information, we've been able to help the development organizations we support to keep their people and their positions aware of the changing nature of the threat, both geographically and from a tactical perspective, from the likes of ISWAP and ISGS.

CTC: When it comes to the Islamist terror threat in the West, does this same approach work in terms of being able to see the direction of travel, with regard to the threat of directed, enabled, and inspired jihadi terrorism?

Winter: Absolutely. Just as people in Syria and Iraq who are supporters of jihadism are knocking around in online spaces, so too are people in the U.K., Germany, and elsewhere. There's a huge amount you can learn from digging into how, at an audience level, these communities are responding to developments on the global stage as well as at a very tactical level, when people are saying, 'I want to go and attack X, Y, or Z' on the basis that it's Ramadan and there's a massacre happening in Gaza. The way that jihadist terrorist ecosystems operate these days is you have geographically very dispersed communities that all operate within the same ecosystem. So, there's a push and pull with as much going into the Middle East as is coming out of the Middle East—especially when you're thinking about ISIS core.

In terms of intent to make *hijra* [migrate] to places like Afghanistan or Somalia or on occasion to Iraq and Syria as well—a much rarer thing these days—it's possible to tap into the information domain and understand the extent to which people in the West are truly, actively, and genuinely considering whether *hijra* to these places is a good idea or not any more.

So, in terms of the threat faced to the U.S. or the U.K. or the West more broadly, there are absolutely indicators in publicly available parts of the internet. Yes, they may be hard to reach. Yes, you may need to know where to go to access them and identify them, but absolutely there are indicators of the intent and broader morale of these communities.

One thing that we've done a lot of work on lately is digging into the way that reports of the various ISIS leaders in Iraq and Somalia being killed have impacted at a rank level or at a supporter level in the broader ISIS ecosystem. We can dig into indications of dissonance or concern within these ecosystems to see whether there is any way to corroborate who these guys are and if they do hold the positions that they're said to hold. And more importantly, at a strategic level, we can examine the extent to which the disruption or degradation of the ISIS leadership has had or is having tangible impact on the group and its supporters—wherever they might be.

CTC: When it comes to the jihadi threat, based on all this data coming into you and your analysis of it, what are the geographic areas that are most concerning to you?

Winter: I would say, in no particular order—just because I can't rank them, because I think they're all very pressing—Syria, Afghanistan, and Somalia. Syria because it is in a period of extreme flux. The transition government is, I believe, making a meaningful effort to conduct a transition, but that's easier said than done when you have the pedigree that the transition government has. Easier said than done under the weight of sanctions that Syria still faces. But we're also in a period where we know ISIS, which has very deep foundations in Syria, is not flexing its muscles there yet. I worry that it is more a question of *when* rather than *if*.

CTC: Analysts have highlighted the fact that since the fall of the Assad regime in Syria there has been a significant drop in ISIS activity in Syria,[a] and I think back to what you said about Afghanistan and the ISIS activity dropping there, before the attack at Kabul airport. So, what you're saying is 'don't assume that that lull is because they are a diminished force. It may well be that they are gearing up to something, and in fact, it sounds like your analysis is they *are* gearing up to something.

Winter: I think it's always important not to ascribe too much credit to actors that may just fundamentally be failing, but I also think it's important not to misinterpret inactivity as a sign of weakness or incapacity. So, especially with the U.S. drawdown, especially with the prospect of further instability, fragmentation, and regional conflict more generally, I think we have to keep open to the idea that

a "In 2024, ISIS was resurgent in Syria, conducting an average of 59 attacks per month, but since Assad's departure on Dec. 8, 2024, its operational tempo has fallen by 80% — to just 12 attacks per month, on average. Even more significantly, the deadliness of ISIS's attacks has plunged by 97% — from an average of 63 killed per month under Assad in 2024 to just 2 per month since then." Charles Lister, "ISIS is on the ropes in Syria. A successful transition in Damascus could deliver a knockout blow," Middle East Institute, April 14, 2025.

"The city of Mogadishu and its environs is increasingly being cut off from the rest of FGS [Federal Government of Somalia]-held territory by concurrent al-Shabaab offensives in the areas around it."

actors that may not be particularly active are *waiting*. We know that it's a time-worn thing that jihadist organizations in particular like to say that they don't operate in four-year democratic cycles. They can wait, and they do wait. So that's what concerns me about Syria.

With Afghanistan, everyone knows about the threat that ISKP presents from a global perspective, and absolutely, from a global perspective, it is extremely problematic. But I think there is more going on in Afghanistan than meets the eye in terms of what ISKP is getting up to. I don't think it's useful necessarily to think of organizations or movements like ISIS solely as militant actors. There's a lot of non-military, non-violent stuff that happens behind the scenes that ultimately facilitates the violence that we all hear about. In relation to Afghanistan, we have individuals in the U.K., for example, that have attempted to make *hijra* there in the *last year*.[1] You don't make *hijra* to somewhere where you can't make *hijra*. If you are a woman seeking to go there with your children and you are a believer in the ISIS creed and methodology and approach, you're not expecting to go and fight. You're expecting to go and live and participate in the civilian project that ISIS has undertaken. So, the fact that we still have people seeking to make *hijra* to a place like Afghanistan, where the Taliban are putting a lot of pressure on ISKP, to me suggests that there is more going on there than just the purely militant facade of the organization that we hear about either within Afghanistan itself or projecting itself into Iran, Russia, or the West.

Somalia, I think, is the clearest and easiest one to situate in this trio, just on the basis that al-Shabaab has been making very significant gains around Mogadishu over the course of the last few months—especially since the start of Ramadan—and we saw the attempted assassination of the Somali president a few weeks ago in Mogadishu itself.[2] But, more importantly, the city of Mogadishu and its environs is increasingly being cut off from the rest of FGS [Federal Government of Somalia]-held territory by concurrent al-Shabaab offensives in the areas around it. So, my outlook for al-Shabaab isn't great—it is slowly and steadily making big gains in the context of a concurrent drawdown in support for the Somali security forces.

CTC: Let's get back to AI and the LLMs that you use and what you've learned about what the AI in this context does best, and what is best left to the analysts in your organization.

Winter: We hear a lot about how AI is changing the world, and sure, it is. But it's not any fix-all situation. It is not yet capable of human cognition or human expert-level analysis, but what it can do is enable an individual analyst to cut not in half but into 10 or 20 the amount of time it takes to generate a reasoned assessment of a dataset that would otherwise be impossible to—in an objective, replicable, and auditable way. Using AI in a constrained way to help parse, clean, process and visualize the hard-to-reach data we're getting our hands on opens up a world of possibility in terms of intelligence analysis that is—we believe and the people who we work with believe—so much more effective and fit for purpose than if your analysts are stuck collating others' assessments of data that they can't see or working with data that, by the time it reaches their facility or the place that they're working, is no longer relevant to what's happening in the here and now.

Being able to bring—again, in a constrained way—technology to bear in this environment is transformative. It minimizes the time spent on necessary but low-value tasks, such as individually coding data points or pulling together visualizations, and maximizes the opportunity for analysts to do the stuff that matters most, and that machines definitely can't and shouldn't be doing. That's where I think technology has really changed things.

Using ExTrac *now*, I could do my PhD in about five minutes, but it took me four years to do it not even 10 years ago. The key thing is the ability to parse data at scale while still being able to jump right back into the weeds and see, and audit, the raw, original data. What's more, the way we use technology means that anyone doing this kind of work today can do so in such a manner that the impacts of human error and subjectivity are mitigated—this is all enabled by mathematical processes that can be audited, that can be replicated, and that can be tested and calibrated to such a point that we know they are capturing and reflecting as much of the data as possible in as faithful a manner as possible. This is what technology enables now. CTC

Citations

1 Editor's Note: "Stratford woman jailed for terrorism offences," Warwickshire Police, April 10, 2025.

2 Editor's Note: "Saudi Arabia condemns attempted assassination of Somali president," Arab News, March 19, 2025.