A View from the CT Foxhole: Greg Hinds, Former Director of Counter Terrorism, Interpol

By Joe Decie

Greg Hinds is an Australian Federal Police (AFP) leader who served as Interpol's Director for Counter-Terrorism in Lyon (February 2021-January 2026), overseeing Interpol's global counterterrorism strategy and its three sub-directorates (Operations; Capabilities; CBRNE & Vulnerable Targets) for 196 member countries. Previously, Hinds spent three years in Liberia as Head of the UNMIL Police Component and Police Commissioner, leading 2,000 staff to build Liberia's police capacity until the United Nations handed security responsibilities back to the Government of Liberia in June 2016.

Hinds' AFP career has spanned Counter Terrorism, Crime, International, Protection, Aviation, Intelligence, and Community Policing commands, and he now works in AFP's Global Operations Command focusing on domestic security against serious organized crime and terrorism.

CTC: What is the toughest CT issue or challenge you have had to navigate through over the course of your career?

Hinds: There's a couple of things that come to mind here. One, from an operational perspective, is the salad bar of ideologies that motivate/drive/influence terrorism today. We're not dealing with the structures that we once did, and terrorism and the threat landscape have evolved. So, this has an impact on how we think about and respond to a threat environment that is guided by much more loosely connected structures—the gamification of and the desensitization of violence, even offenders becoming much younger.

Due to these changes, we too have had to evolve, and at times we probably haven't matched that pace of evolution with our ability to shift policy, to shift legislation, and to shift our operational responses because their adaptation has moved much more quickly than ours in recent times. We need to think about how we bridge policy—national security and foreign policy, counterterrorism policy—with an effective operational response. My time at Interpol, given its position as being a voice for global law enforcement, gave me unique insights into this issue. Members of Interpol have a common agenda, but each country brings its own mix of capabilities, policies, and approaches, and that can make it challenging to unify and synchronize efforts and activities. For example, of the 196 member countries who are working CT every day, how do we make sure that we're equipping them with the necessary tools, resources, and resource mobilization that they need to actually counter the threat?

Another challenge that I have observed, particularly during my time in the U.N. and also my time at Interpol, is what it takes to build capacities and capabilities, and make sure those are fit for purpose. Given the mix of capabilities of various countries, this requires an ability to adapt.

For example, a lot of our neighbor countries don't actually have mature operating [CT] models, mature resources, equipment, and those sorts of things. Some of them don't have power, some don't have computers, and yet, we see that what has been going across our online environment has been very problematic, as it serves as a means of either moving resources, recruiting, [or] sending finances. If you don't have these basic capabilities to operate and act in that type of environment, how is it that you can make their responses fit for purpose? How can these types of countries absorb or learn from what mature entities are looking to do/are doing? Because, as you know, we're only as strong as our weakest links, so I think this was a challenge.

CTC: So, when we look at the capacity, capability, and expertise challenge, which is a component of what you laid out, how do we address that from a partnership perspective—whether it's bilateral in your home country or in the U.N., the D-ISIS coalition, or Interpol?

Hinds: What we've seen is that we have to look to non-traditional partners. We have strength across our law enforcement and our national security community. Our intelligence, our military, and our law enforcement work quite well together, and our interoperability works well because this is stuff that we've rehearsed, exercised, and tested. But there are also challenges. For example, how do we make sure the right information is in the right hands so people can do their jobs? From the lens of Interpol, a core part of our role within the global law enforcement community, was focused on having a sound global security infrastructure specifically exchanging information, so we could make sure that the operationally relevant information is sitting there so we can best support member countries in preventing and responding to the threat.

When it comes to partnerships, there are also issues in relation to what capacities and capabilities exist. If we looked at R&D [Research and Development] across the globe in relation to what we do around strengthening security, strengthening our responses, looking at analyzing data, if we just tapped into that a little and we shared capability across the globe, we would find that we'd actually harmonize and uplift our ability to do this. Typically, we're doing it individually.

This comes back to trust and confidence in what we're doing. How do you make sure that we're doing this for the right purpose? It's not necessarily about disclosing our human sources or our information or our specialist capabilities, but there is capability that's cutting edge in relation to analysis, our resourcing, our databases, our training, those sorts of things. How do we make sure that we're doing a better job across this cohort of relationships in various areas to maximize what already exists and ensure this is in the right hands to make the right decisions?

When it comes to multilateralism, we need whole of society, whole of government, whole of non-government mixed together. And so, similar to what we're doing at a national level, that needs

Greg Hinds

to be amplified at the regional level. We also need to do that at the global level.

Risk dynamics are an important factor, too. We don't want to see a bomb go off and then go, 'That was a pretty good bomb.' Our risk appetite is that we want to prevent this from happening. So, how do we disrupt ahead of time? We want to be much more in that disruptive, preventive space. Being in that space means that we need to fight against complacency and make sure that we're really invested in this because we have to be on our game 365 days of the year. Terrorists just have to be lucky once, and we saw that here in Australia with the Bondi Beach attack.[1] Effective partnerships and information sharing that are fit for purpose help us to navigate that crime puzzle.

CTC: Cop to cop, agent to agent, that is a more organic piece. How do you see the current challenges on national-level assets? Whether it's ASIO (the Australian Security Intelligence Organisation) or other components, or even from an Interpol perspective, how you would see that flow of data and are there current challenges with that? What are some of the best practices that you have seen to ensure that happens?

Hinds: I think the biggest thing is, how do we leverage the capacities and capabilities of different entities? How do we benefit from the comparative advantage that we collectively bring? If I have a look from an Australian perspective, we bring states and territories together across the policing space. We also bring in our national security agency, and the whole idea is how do we make sure that there is productive convergence around a national security/terrorism threat. Has there been criminal offending involved in that? And how do we then make sure that we're not compromising each other's information, but we're actually being complementary to each other's goals at the end of the day, while also leveraging our powers, our experience, our expertise.

That's from a national sense. If we then expand that globally, how do we make sure we're replicating those sorts of practices at the end of the day? It's the information sharing which is key to this, making sure that all the information that's available is in the right hands so that the right people can make the right decisions at the right time based on their ability to do their jobs. That's what we're looking to do. And for most of us, particularly in the global security architecture, we want to make sure that's at the frontline. How do you stop threats at their source? So, if we don't want terrorists moving across borders, we don't want lots of harmful goods, equipment, money, firearms, whatever it might be that supports terrorism moving across borders, [then] how do we make sure that information is shared across and between nations. There's not too many systems that allow that. Interpol has a global system that connects to its 196 member countries, pushing those systems out to those border locations so that those key decisions can be made about people who are wanted as part of an Interpol notice; how to handle an extradition process; or blue notices around persons of interests, handling green notices focused on intelligence, or purple notices focused on *modus operandi*, so that you're actually in a better place to actually understand threat dynamics and how it might be crossing borders and how best to respond [to] and prevent it. If warranted, Interpol will also issue an orange notice to notify and highlight immediate threats, and how a nation or community might best respond.

Those mechanisms, which help to make sure that we are sharing the information at the right time and getting it to those people that that have the right and need to know, are really important. Trust and confidence in our systems is important, too, and we need to make sure it is guided by a common agenda, a common goal, and that we are working to operationalize together. A key to integration is bringing partnerships across the military, the security services and placing those together, building cohesion around those sorts of things and making sure that we are doing this systematically.

CTC: You have talked about the importance of coordination and information sharing, and different partners being in different places when it comes to their capabilities and capacities. Can you add some more color about how Interpol does that from a big headquarters?

Hinds: We all talk about [how] we're very global in our outlook and those sorts of things. But when you are the global agency, it is a very different lens looking at how you do it. So, no longer was I an Australian [in these situations]. I was there as an Interpol employee, one of the senior executives. If I look to the current Global Coalition Against Daesh's priorities as an example, they've looked at three thematic priorities: One of them was stopping terrorist travel and mobility; another was stopping their financing, their funding mechanisms and streams; and the other was around their online communications. How do we make sure they're not looking to radicalize and recruit? How do we also make sure that they're not actually looking to prepare operations and so forth? So, if you looked at those particular things, if we got those right, that's a sound approach to disruption globally in relation to that.

The challenge here is how do we mobilize resourcing so that 196 member countries benefit from that. Now, not all 196 will need investment because they're already self-invested, but there is a large part of the globe that needs investment in relation to this. So once again, how do we understand the threat environment? By understanding the threat, we can then prioritize on how best to respond. Is that through technical means? Is that through capacity-building? Is that through equipping?

One of the important things under my leadership when it came to building capacity is that we needed to make sure we operationalized it. We wanted to make sure that we weren't just doing stuff to look at things like skills uplift. We wanted to make sure that we were doing things at both the individual and the institutional level. That is because it is part of the sustainability piece. We also wanted to make sure those efforts are feeding into national systems, regional

systems, and global systems. Because it's a global problem. This helped to lead to a more informed approach that aimed to stop threats at their source.

Oftentimes, we would bring member countries together on a common endeavor because they didn't know how you actually bring those people together. Because we could see it, we were able to bring member countries together on a common cause so that the pieces—the broader pieces of the crime puzzle—could come together and they could work on this together. That was a key role of Interpol, as well as being a neutral, trusted partner given that this is a part of the organization's constitution.

But of course, one of the challenges is that the organization only deals with non-state actors. We don't get involved in anything that's racial, religious, or of a military nature, or is political. So, we just want to make sure that we're doing things that are in the best interest of our constitution and the best interest of the member countries concerned.

CTC: You mentioned a lot of critical partners, but how do you get to a common understanding, a common approach, when the counterterrorism mission set may no longer be the top priority? I imagine some of your resources over the last two and a half decades have probably gone down. You deal with a diverse mix of partners who have somewhat aligned agendas, but you also have to navigate unique national or regional circumstances, set against a diverse and dynamic terrorism threat environment. How did you thread that needle?

Hinds: For us, a grounding principle is that we saw that we were a critical voice for global law enforcement. But how do you make sure that the voice of law enforcement is being heard? Because the forum which we were in was typically not a law enforcement space. So, we wanted to break down the mystique of Interpol. It's not what you read in novels and what you see on TV. Whilst we do some really sexy stuff, we are one layer removed. For example, I didn't have arrest powers. So, therefore, it's important for us to consider how we can make sure that we're actually equipping our members as best we can to actually defeat the threat. The approach that we took there is that we want to build individuals and institutions and get information in the right hands. That was critical for us.

One recognition was that we were not looking at sustainability of the effort. It is like having an ashtray on a motorbike: If we aren't thinking about sustainability, it defeats the purpose. So, we wanted to make sure that we were looking at creating dividends and that there was a return on investment, and also that people understood what they were investing into one from a partner sense. But also from a beneficiary sense, too, you can't regionalize the globe to actually make it a secure globe.

To be sure, we have some really strong Pols around the globe, such as Europol, but not all of them are mature. For example, if you're coming into Europe, one passport check would actually check national systems, Schengen systems, Interpol systems. Therefore, our members were getting a much better dividend to help them stop threats at their source. You had information and frontline decision makers to apply the appropriate responses that were fit for purpose in relation to people or goods moving through borders, and those sorts of things. Emphasis was placed on how you replicate good practice across the globe in relation to those sorts of responses.

When it came to our capacity-building efforts, we had former employees with the subject matter expertise who understood the operating environment. So, that cooperation/collaboration piece was really strong. How do we bridge what's happening across military, security, and policing environments, and also there's a greater law enforcement community that policing is an important part of.

One of the other things that comes to mind is the polycriminality nature now of crime. Polycriminality is one of the reasons why I went to the General Assembly several years ago and said we need to have an all-of-crime approach to stop terrorism in all of its forms. It was really important for us to make sure that the cattle rustling that was happening in Africa and was actually generating funds for ISIS core is actually seen in the proper context because the upstream and downstream effects of that vary. The illegal logging, the illegal mining, all those sorts of things, if you don't understand the context of the crime, you don't actually understand the ramifications of it, which is why we said we need to think differently about the criminal environment.

We also need to actually understand the criminal environment differently because it imposes different thinking, which leads to different approaches that can enhance disruptive efforts. Understanding the context of the criminality will best shape how we respond and what tools, resources, and expertise are required. We know, for example, that the trafficking of drugs is also a fundraiser for these sorts of things, and supports the movement of people and goods. The facilitators are much more blurred these days than what they once were. I might have gone to one person for my money. I might have gone to another person because he got my firearms. These days I just go to that second person for everything because he's quite happy to move anything. That blurring of facilitation and movement has an impact on terrorism, and what supports and enables it in different contexts can be very different, and different across time. So, therefore I think we need to have this whole of crime approach, which means that we need to then think very differently about our crime and our terror environment.

CTC: How does Interpol deal with volumes of data and the exploitation and then optimization of all that data through initiatives such as Interpol's Project CT tech?

Hinds: At Interpol, we had a CT-focused crime analysis file, and it had something like 200,000 different profiles of terrorists in there. There were about 1.3 million pieces of data related to terrorism and terrorism entities. Realistically, that's probably only a small fraction of that type of data held on a global level, but that's what's been shared with Interpol to help us connect the dots. And so, one of the key elements is, how do we complement that type of data?

Most crime is transnational in nature. At Interpol, we should be someone that you're consulting with in relation to these sorts of things, because no one knows everything. And the information that one partner may need is probably out there, but it may not be clear where that data resides. So, you have to make sure that you're interrogating the proper datasets where this stuff exists; if you aren't, you won't actually get the fuller picture to help you make informed decisions. So, for us, we were trying to create a funnel and a space in which people could actually share this information and to better connect that data with investigative actions.

As part of these efforts, we provided a 24/7 service to our membership that allowed members of our crime analysis file, which

is a unique data set to CT, to seek Interpol's support whenever they might be having an active investigation, a cold-case investigation, whatever it might be, so that we could help them understand if the person or entity is known. This helped us to identify common interests or areas of overlap. For example, we may even, depending on how the information is shared, turn around and say, 'Russia, you and the U.S. actually have an entity of common interest.' And to be honest with you, the U.S. and Russia were our biggest data contributors to this CT data file. So, not always do we have the information, but with our bilateral and multilateral partners working together, Interpol brings that collaboration together in a way that there isn't perhaps the antipathies that may exist at a bilateral level. Interpol was working to support the common endeavor where and when we can.

CTC: At Interpol, when you are dealing with 196 different countries, how do you have a common lexicon?

Hinds: One of the things that was very difficult when I was in the U.N. was that the U.N. didn't have a definition of terrorism. Interpol doesn't have a definition of terrorism either. And we didn't need to. Why? Because we supported member countries with *their* definition of terrorism. So once again, we didn't try and create 196 member countries' ideas of what terrorism might look like because you can imagine just how complex that is. What we looked to do is, how we can actually help them operate within their space?

We tailored our support based on their legislative and policy frameworks, and so that makes it a little bit easier. We didn't try and over-engineer it. We didn't try and complicate it because I think it's more about complementarity, more common approaches focused on continuous improvement. We were also looking at gaps. We were looking at vulnerabilities and how people can look to strengthen those based on our experience and exposure helping them do it within their own national frameworks.

CTC: Fast forward three years from now: What resource, policy, or threat after do you think is going to keep you up at night? And what can we do between now and those three years so that nightmare does not happen?

Hinds: I think the dual use of technology, the pace of technology, the automation of all that is a real problem because it's a tool for good *and* it's a tool for evil. But we also find that the adaptation for evil is probably much quicker than what it is for good. So, that concerns me.

I think also about the weaponizing of CBRN materials: We're seeing a very different actor in this particular space, whether it is quantum physics or synthetic biology, all that sort of stuff. We've been fortunate we haven't seen this advanced in weaponizing terrorism, but we saw the impact and potential of it through the lens of virus outbreaks and disease. For me personally, I saw the impact of Ebola when I was in West Africa, and we all saw what happened with COVID. If you successfully weaponized a virus, it could have global impacts that are just phenomenal. So, when it comes to the CBRN space, and whilst we have people focused on and looking at it, we're probably fortunate that as far as threat goes, we haven't really seen capability and intent come together. Some people have the capability, some people have the intent but haven't got the capability. So, we've probably been fortunate we haven't seen an augmentation of such a threat.

The other issue that keeps me awake is the cyber threat. The fact that we haven't really seen this play out is a good thing, but we've seen what happens when the power goes out in hospitals. We understand what happens if it goes out with aircraft traffic controllers and those sorts of critical infrastructure. We understand the impact on our daily life when something like that fails.

So, our critical infrastructure protection, the weaponizing of CBRN, the ongoing challenges around technology, AI and what that will be used for in its adaptation, they're the things that we really need to prepare for next. That does not mean those types of attacks will necessarily be the most sensational attack. Recently in Australia, it was two men with guns and that was our crystallizing moment of change for us here. When it comes to what may come next, it may not be planes into buildings. It may not be taking out vessels at sea.

We need to pay attention to incidents that can change the psyche of government, of policy makers, of legislators, that require and invoke change because we've become comfortable in our space. To be honest with you, when I was at Interpol, I said, 'We are one attack in a Western city away from a real shift in CT policy.' Today, the nature and type of people that are involved in extremism, and the salad bar of ideologies and options available to people, make things really difficult. We've now got legislation in Australia around hate crime and symbols and those sorts of things where we didn't have that before, but it took a terror event to do that. It wasn't as if we hadn't thought about it. How do we future-proof our environment so we're not playing catch up and we can learn better from others in relation to our responses rather than having to go through the pain of a tragic event to facilitate change? CTC

Citations

1 Editor's Note: Andrew Zammit and Levi J. West, "The Bondi Attack: The Islamic State's Strategic Shifts and Jihadi Tactics in Australia," *CTC Sentinel* 19:3 (2026).