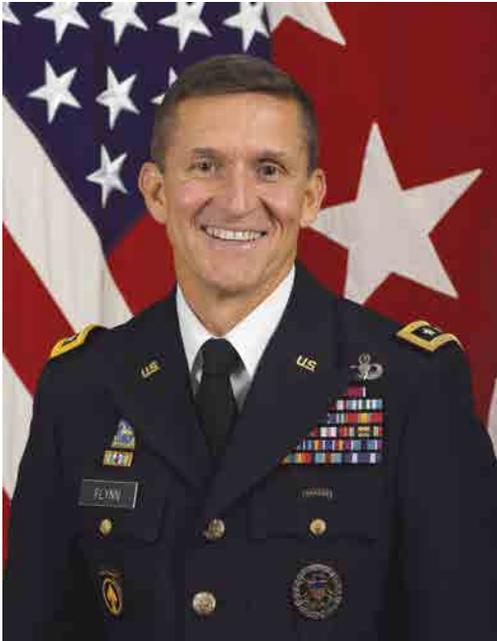


# An Interview with Lieutenant General Mike Flynn



*In 2010 you co-authored an article "Fixing Intel;" what was wrong with intel when you wrote that article?*

Flynn: In 2009 I was on my third assignment in Afghanistan and we were in the process of implementing the new strategy that was going to be very population centric. When I looked at the intelligence system, as the Chief Intelligence Officer for the International Security Assistance Force (ISAF) and U.S. Forces Afghanistan at the time, I realized that for us to be successful we had to refocus on the right aspects of the environment. What we were focused on was to a large degree - I would say 95 percent - the enemy networks (e.g. Taliban, the Haqqani Network, etc.) We had tremendous fidelity on those because we had been studying them for years.

What we quickly realized was that we had no knowledge, no real understanding of the various tribal elements within Afghanistan. We had to understand the cultures that existed, the dynamics of the type of government that we were trying to support and the population centers that we were actually operating within. We honestly did not have any deep understanding of any of that. We were trying to figure out who was who, from the local governments on up to the national government, and we did not have any captured data, information or knowledge. Frankly, we did not have an understanding of the people who had been coming in and out of Afghanistan. We did not have that real depth of understanding that we had in other places - in Iraq it took us a while to get there. That led me and two colleagues to sit down and put our thoughts together to say we needed to do something different; we needed to completely realign our focus to the population and to the build out of the Afghan national security forces. That is when we described the color system, the red, the white, the green, and the blue. The red was the enemy; white was the population; green was Afghan national security forces; and blue was us. We had a really good picture of the red and the blue. We had no picture of the green or the white, and it was really stunning; so, we decided to put our thoughts down on paper, but we were not sure at that time how to get those out into the wider community.

*That article had fifty thousand downloads within a fairly short time. Would you consider, three years later, that intel is now “fixed?”*

**Flynn:** No. In fact, just the phrase “intel fixed” is flawed. Intel is constantly changing because the environment is constantly changing. Because of steps that were put in place and the training that was changed back in CONUS at various training centers (the Army’s Joint Readiness Training Center at Fort Polk, Louisiana; the Army Training Center; the National Training Center at Fort Irwin, California; the Marine Corps training Centers, both at Pendleton and Lejeune), when units arrived in Afghanistan they were able to adjust to understanding the local population, the Afghan national security forces, and the governance that we were trying to help support. They also sought to continue to understand the enemy that we were facing. Initiatives were taken in both CONUS and in Afghanistan. The Civilian Operations Intel Centers (COIC) that we created were very helpful for the ISAF Joint Command (IJC). But ultimately, intel is not yet fixed. We are better at it, but it is a constantly changing environment.

*What are the obstacles to fixing it? To fixing the flawed processes?*

**Flynn:** The number one obstacle is culture. Our challenge is changing the mindset of our military forces. We have to make sure that our military forces—our Marines and our Soldiers, principally—know that they are coming into a combat environment and that it is a dangerous environment, so they have to focus on the enemy. But in order to be successful and in order to actually shift the environment back to the Afghans; we had to understand the

population that we were in fact operating amongst. We also had to understand the Afghan national security forces that we were building and then incorporating into that environment. That was really a difficult thing for many to come to grips with. Culture was probably the most difficult thing for us, specifically our culture and getting us to think differently about how we operate within the environment. If there is a lesson learned from this whole decade of war, it is that our failure to understand the operational environment actually led to a mismatch in resources and capabilities on the battlefield and how we applied them. Once we got over the hurdle of culture and asked, “Why do we have to do this?” people who actually understood the problem realized it. In some cases, commanders made the change because commanders can change the training, and can change how the military trains forces to prepare, advise, and assist. So instead of combat forces, which are what we had in the 2009-2010 timeframe, we shifted to advising and assisting forces. These require much more knowledge of the white and the green. In fact, that has been our whole focus in these last couple of years.

*Our conversation has focused on Afghanistan and by implication, Iraq. Would you say that these problems you identified in 2010 and the solutions you are discussing now are globally applicable?*

**Flynn:** Absolutely. Since that publication I have personally, by working with partner nations, spoken about this issue and now other nations are incorporating those ideas into their own country and regional contexts. It is about understanding the human environment inside the contiguous boundaries of

individual countries and inside this seemingly boundary-less world within which we now find ourselves. In addition, simply in terms of measurement, “Fixing Intel” has been translated into a couple of different languages, one of which is Russian. There is another application of “Fixing Intel.” The idea has a lot to do with the integration of intelligence operations and law enforcement operations. We have spoken to law enforcement agencies about how they work with intelligence and they actually are, in many cases, applying the principals found in “Fixing Intel;” it has had a broad impact.

*One of your priorities coming to the Defense Intelligence Agency (DIA) was the institutionalization of intercultural analysis. What motivated you to make that a priority? And how have you approached integrating those capabilities within the DIA and the broader intelligence enterprise?*

**Flynn:** This is a really interesting field because it has come out within the last 10 years, and for me personally it has had an impact, which is why I am making such a big deal about this. It has really been over the last 30 or 40 years that the changes and the shifting in the societies and the demographics of some of the most difficult places we have to deal with (Central Asia, the Middle East, North Africa, and Southeast Asia) have been occurring. Specifically, I will talk about the regions of Africa, North Africa, the Sahel, and the central African states. In some of these places there are challenges with governance, challenges with lack of governance, challenges with under-governed sanctuaries where militias exist, challenges where insurgents exist, and challenges from terrorists who can protect

themselves, all compounded by the huge growth in populations over the last 30 to 40 years. And so we have nations with large segments of populations, and populations comprised of a lot of young men, but with not-so-huge economies, that are going to turn to things such as transnational crime, narcotics, human smuggling, weapons smuggling—the kinds of things that converge, that we have to understand and then deal with. So the convergence of terrorism, the convergence of insurgent groups, the convergence of militia groups that are all coming together as well as these transnational, organized, well-funded criminal activities have not just regional aspects behind them, but have global aspects with which we are going to have to deal. So the advent of socio-cultural analysis, the understanding of the human domain and the human environment is critical to our ability to be able to operate, support, engage and partner with some of these countries. Also, when we look back at ourselves, we have to consider how we design the force, how we structure our forces and the capabilities that we need to operate in this new, rapidly changing environment. I will tell you that intelligence, special operations forces, and cyber are three components that we want to apply in very different ways in this phase zero environment, or pre-conflict environment. There are aspects of all three of these capabilities that I think, if blended together, can help us stay out of conflict and help other nations protect themselves.

*Are we now systematically collecting intel on populations and local socio-political dynamics in regions of interest?*

**Flynn:** I would not use the word systematically, but I would say that we are prioritizing

the kinds of collection that we need in order to understand the environment. We are also working with new, and expanding our existing coalitions or allied partnerships in different ways. We are definitely sharing information with many more new partners these days than we ever did in the past. This is information that is readily available to us, and our intelligence capabilities have matured to a point where we are very capable of gathering this kind of information and then working with our close partners, analyzing and assessing an environment, so we can help some of these partner countries do different things with that information; for example, understand the best places to begin health projects, the best places to build schools, and the best places to conduct irrigation projects where segments of populations exist without tribal boundaries. We have to be careful of that, because we, in our culture, think that if we want to get two tribes to work together, we should build a well right in the middle. That is not necessarily what we should do. Instead, we should give them the shovels and give them the where-withal to be able to build their own wells. They know how to dig—something we witnessed in places like Afghanistan where we were trying to think strictly in our mindset about how to bring people together. And in fact, that is not the way certain cultures prefer to interact. So in fact, the answer to your question is yes, and I think it is going to help us out quite a bit in the future.

*What is the relationship between intel and open source information? And how can the two be seamed together to give national security policy-makers a better, more holistic understanding?*

**Flynn:** That is one of the misunderstood capabilities. Intelligence is analyzed information; it can be information reported by sensitive human intelligence, sensitive signals intelligence, sensitive geospatial intelligence, or even open source information—which there is a lot more of these days, far more than there is of all those other types of information that I just mentioned. It is then analyzed and turned into intelligence. Intelligence is actually supposed to provide the meaning of all this noise out there in the environment. Now all that said, in 10 years, and I will just use my own experiences, ten years ago 80 percent to 90 percent of what I provided to my commanders when I was a division or army corps G-2 or JTFJ-2, would come from sensitive intelligence sources. Approximately 10 percent, maybe even 20 percent would come from the open source environment. But today, that has completely reversed. Today, I am guessing a little bit but I have seen some hard data on this, and about 70 percent to 80 percent of what I am providing to decision-makers is actually coming from the open world. The sensitive information is really at about 20 percent to 30 percent. It has completely reversed in about a decade. Think about how social media sites like Facebook did not exist until about February of 2005; today there are over a billion people using Facebook. Twitter was simply a sound in 2005; today it is how people are communicating. LinkedIn is another social medium out there. We have all these new media for information creating noise, but it is also the environment telling us about things that are happening. I can follow Twitter on my personal iPad and see volumes of activity. Being in the intelligence field, as a means of intelligence production, I need to be able to incorporate those kinds of information feeds to then turn the information they share

into intelligence and give decision-makers meaning to what is happening in the environment. That is a huge change. I have grown up in a closed-loop system and for 20 years of my career that was probably okay, but now we are in a completely open world, a far more open world than we have ever been in, and the intel community's closed-loop system has to adjust. We have to adjust to this new open world. If we do not adjust, then we are missing what these new voices are telling us.

*How does that particular change, the exponential increase in the number, the magnitude, the volume of information sources, complicate the intel community's work?*

**Flynn:** It is an immense complication. There is so much information; for example, we have the ability to download as much information in an hour today as we could download in all of 2004. That shows the magnitude of information that we are able to absorb and now we really have to scope that information, to figure out what it all means, because most people will say, "How do you know what you're doing? Is there too much of it out there?" So it really does require us to do a lot more prioritizing and to be much more precise in whatever we are looking for. In the past we could get away with very imprecise Priority Intelligence Requirements (PIR). We could get away with less-precise questions just 10 years ago, maybe even five years ago. Today you cannot get away with imprecise questions. Our ability to get precision out of all the noise, out of this scale of information that is out there, is much better if our questions are more precise. The other aspect of this is how technology helps the analyst in this new environment. We are exploring this and developing our outreach

primarily to private industry. We are developing technological tools that allow us to do much better triaging of information and information feeds that are coming in. We are now vastly better than we were as recently as three or four years ago. I was in Afghanistan in 2009 and 2010 and as we sit here today I see that that environment, as well as our technological abilities, has also rapidly developed to help analysts get all of this information. How do we figure out what it all means? There is some technology that helps our analysts with that, but it still takes a uniquely-skilled, well-trained, intelligent person to be able to decipher what it all means.

*In this environment, is institutional stove-piping - or compartmentalization - still a problem?*

**Flynn:** It is less of a problem, but it is still a problem. We are better; we have made great progress in integrating our capabilities, in integrating our people. We still have some challenges in integrating our technologies, in integrating our communication systems. In the past there was some intention not to share; that is no longer the case. The intention is now to share instead of attempting to work in our own little system. There are still some hurdles because there are still some very sensitive things that need to stay sensitive. But the leadership, from the President on down, has every intention to increase the sharing of information and intelligence. We are working on building bridges to each other in our own systems, in our communications capabilities, and in how we put processes in place to ensure that we are sharing everything that we possibly can. Because I am asked sometimes, "What do you think are the biggest threats out there?" The

biggest threat to us is our inability to work together. I think that everybody recognizes that if we do not work together, we are going to have failures in our systems. I would say 99.9 percent of people would say, “Absolutely. We want to work together. We want to integrate. We want to build the systems – to put the systems in place so we can work together better, and share information.” But there are going to be things that are going to happen and we are going to find breakdowns or weaknesses in our system; but it is no longer intentional.

*Does that intention to share extend beyond the intelligence community to other agencies as well? Or is it restricted to the intelligence community?*

**Flynn:** Within the U.S. Government, there are non-intel community partners with whom we have done a lot of great work. One thing that is not really well-known is our work with what we call the Non-Title 50 (NT50) crowd; members include the Department of Commerce, Department of Agriculture, Federal Communications Commission, Social Security Administration, and Transportation Administration. One of the benefits of having the Office of the Director of National Intelligence (ODNI) is that they have discovered this other segment of our government that has an enormous footprint globally. Health and Human Services for example monitors health and disease world-wide. The DIA has the National Center for Medical Intelligence so we have developed this capability internally when in fact we have an entire government structure that does health and human services globally; we are working much more closely with such organizations. On the operational side of our military forces, I would

say that the fusion of intelligence and operations is probably one of the biggest lessons learned out of the last decade of war. This idea of operations and intelligence fusion is one of the lessons learned from the battlefields of Iraq and Afghanistan. We are trying to incorporate that lesson in our operational activities both in CONUS, and around the world. There are exercises, combat deployments, and conflict deployments in which we are involved where I see this all the time; it is very good as far as applying a lesson learned from this past decade.

*You spoke about the integration of socio-political, cultural intelligence within the intel community. To what extent are we collecting information and creating intelligence dealing with non-state actors, particularly transnational illicit networks?*

**Flynn:** This is difficult for defense intelligence. Defense intelligence is about understanding nation-state militaries and their capabilities, their intentions, their doctrine, their organization, and their leadership. What you are asking about reflects a really different dynamic that we are facing in the world today. It is not that transnational, organized crime had not been around—the mafia in the early part of the last century was a transnational, criminal organization—but the growth of this threat, and not just in terms of the scale and the dimensions, but also how well-funded many of these organizations are, is a new dynamic. They are funding things like militia groups, terrorist organizations, and other aspects of the environment, such as the global flow of narcotics and weapons. Weapons smuggling is a huge gray and black market driven by large sums of money and very

interdependent and interconnected criminal organizations that are creating real havoc in some regions of the world and challenging countries to stand up strong governments to deal with these organizations. Consequently, on the defense side of intelligence and for intelligence in general, we are going to have to make some decisions about how much we prioritize and how many resources we put against these kinds of organizations. These non-state actors are absolutely impacting the ability of nation states to do their jobs, to govern and to provide security, and to provide the where-withal for the people living in a contiguous country. It is really difficult.

*What concerns me, particularly in times of austerity when we are emphasizing partnership and building partner capacity, is how these illicit networks impact the security of our partners; countries like Mexico, like El Salvador, the Middle Eastern countries...*

**Flynn:** And I would just add, not to identify one country over another, but even in our own country and in our big cities there are transnational, organized criminal groups. Narcotics and other illicit networks now flow through all parts of the world; in West Africa all of the countries from Nigeria to Morocco are engaged—and in Southeast Asia, too. I just came back from Jakarta, where I spent a week with all of my counterparts—essentially about 20 nations’ defense military intelligence officers. We were not talking about big battles at sea, big air operations, but instead, we were talking about the kinds of issues we’ve been speaking of. We were talking about how we can deal with them because they are affecting us like a cancer inside of our system, and we have to deal with it. We have to put the right

medical application against it; we have to use the right kinds of tools to be able to rip it out of the system or at least stamp it down so it does not spread. It can really make things worse for a particular country as it is trying to govern its own population because these networks can be truly devastating.

*The conventional wisdom has it that venally-motivated, transnational criminal organizations would not work with ideologically-motivated, terrorist organizations such as al-Qaeda. To what extent do you think that those two separate kinds of organizations; the criminal organizations versus the ideologically-driven, terrorist organizations and insurgency movements, are converging? Is convergence a reality?*

**Flynn:** Yes, convergence is a reality. The statement you began with is completely false. There are plenty of facts out there and you could do a really good open source survey of a lot of data that exists, clearly linking terrorist and criminal organizations. I define terrorist organizations as non-state actors, regional militias that are definitely causing problems inside of a region and in some cases, taking over whole regions. It depends on where we want to talk about, but whether it is on the continent of Africa, in Southeast Asia, South Asia, Central Asia, Central America or South America, terrorists are dealing with transnational, organized, extremely well-funded, criminal cartels who are helping them smuggle human beings, narcotics, and weapons. Anything that has a price on it, these groups are working together to traffic it. I think that the convergence you are describing is in fact happening faster than we are realizing it. I think that during the first half of this century

we are going to see more and more of this. I see it certainly in the intelligence assessments that I am privy to. I think it is something that we are going to have to make some decisions about from a military perspective, concerning how we organize to protect and provide security for this nation in the next 50 years. It is going to have to be different than what we are talking about today.

*So do the changes that we have been talking about suggest to you that the nature of conflict, the nature of war, the nature of defense, the nature of national security is evolving?*

**Flynn:** I would say that we are going to have to be incredibly agile if we continue to stay the way we are. It is important to always have something in the tool bag—the military tool bag—to beat the existential threats that are out there. But how many tools do we need? Those are the issues being addressed by the Department of Defense. I believe that we are going to be more and more involved in these types of conflicts that we have seen over the last 40 years—from the early 1960s all the way through the last decade. So whether it is just one way of war for the United States to have to be prepared for, or whether it is the new way of war in which we are always going to be involved, I have a difficult time sitting here telling you precisely that that is going to be it. What I see emerging, and back to this idea of convergence, is our way of life being assaulted every single day and it is not necessarily being assaulted by nation states. It is being assaulted by actors who are gaining capability and learning the world of cyber—another converging activity in this non-nation state world. “Hacktivists” that in some cases work

individually, and in other cases work collectively, are damaging our critical infrastructure. Cyber threats are another form of convergence because a hacktivist who is able to steal money from the banking system and then fund threats in the physical world, back to some other type of criminal activity, must be dealt with in a whole new way. From our little world here at the DIA, we are actually looking at a completely new model for training our intelligence analysts. We are going to run a six-month pilot to learn how we can train analysts for the future. We have to start somewhere because it is no longer about order of battle (how many tanks, how many planes, the size of the air field, etc.). It is now about the socio-cultural dynamics of an environment: how many militias are out there; how many tribes exist and what they are doing; what is the size; what is the scale of the tribes and how many countries are there within a region. They do not see themselves with borders. The borders created post-WWI or post-WWII do not exist for many people anymore.

*How has our intel helped national leaders understand the current crises of the day, such as in Syria, Libya, and Mali?*

**Flynn:** I think we have definitely helped our national security leadership understand what is happening, but I think we are still somewhat reactive. Figuratively speaking, after the punch has been thrown, we know what happened, or what is happening. As long as we are able to absorb that punch, which we have been able to do in the past, being in a reactive mode is doable. We can then provide better advice and assistance to help decision-makers make better decisions; to give them an advantage. What we are still really struggling with is

what I would call “preventing strategic surprise.” So part of DIA’s mission for the Defense Department is to prevent strategic surprise. Years ago, we were able to measure activities and events in months, if not years in some cases, and over the last decade that measurement began to shift to days. Strategic surprise is now measured in days, possibly weeks, but if you look at today we are still dealing with the advent of what is going on in Egypt and Syria. Egypt went through a change of government that took place in about 10 days. Trying to understand what was happening—judging it, assessing it, getting the community to figure out collectively whether we agree or disagree—proved our own processes may not be as agile as they need to be in this world where information bombards us. Strategic surprise is a really important element and it is now measured in days and weeks when it used to be measured in months and years. Our organization and our mindset still measures in the longer period of time, so we have to create a mindset and a culture that operates in a much more agile manner. We have to move to a decision, or at least move to an assessment to enable a decision, much more quickly so decision-makers have more time. The less time they have, the fewer options they have.

*So perhaps we could say, as you wrote in an article that PRISM published, “We haven’t yet gotten left of bang.” Another of your priorities when you came here was to create a defense clandestine service. Why is it important that the Department of Defense have its own clandestine service and has there been any pushback to that idea?*

**Flynn:** The Defense Department has always had a human intelligence component

in the department’s overall structure. One of the major lessons learned from certainly the last 10 years, if not the last 20 years, is this need for what I would call a “fingertip feel” of the environment. We absolutely need to have, well-trained, culturally-attuned, language-capable individuals out there in the operating environment who can help us better understand what is going on in these operating environments in which we are likely to operate, not only as military forces but as partnered capabilities with some of the countries with which we are in fact working very closely. So therefore, we have stood up this defense clandestine service, which is an outcome of our former defense HUMINT service. It is not only a name change, but also a mindset change where we are going to be far more integrated with our national partners at the Central Intelligence Agency (CIA); we will be concentrated more overseas than in CONUS where we have had a lot of capabilities planted. Now we are shifting to a more overseas-oriented operation. We are changing the cultural and the language requirements; it is a much more integrated force. I believe in the next couple of years it will be a much more effective force. We have received enormous pushback and have encountered huge hurdles. Some of it has been our own fault for how we have messaged this capability. We have to demonstrate the value of this capability and once we have done that, as we have done over this past year, the more we have been able to show the value, the more we have received support from many once skeptical members of U.S. Congress. I think we have won more and more of them over as we have begun to demonstrate that we are much more integrated; we have a much more disciplined system in place; we are getting more and more people trained at the right levels;

## FLYNN

and we are creating opportunities for ourselves in the future. When I say opportunities, I am not just referring to opportunities for the individuals, but also to opportunities for the security of this nation, for the Defense Department and for some of the new strategies that we have. We are dealing with a doctrine of anti-access area denial. That kind of a doctrine requires that those people who are forward deployed understand the defense requirements we must acquire. The more value we demonstrate, the lower those hurdles become and the less we are challenged in building this capability. If we want to stay “left of the bang,” we absolutely need well-trained, culturally-attuned people in these environments to be able to understand what is happening out there and then feed that back into the system. We are doing this particularly on the defense side. We have a lot of defense partners in other countries with whom we have always worked and so we absolutely want to further those relationships using this capability. The Defense Department can do that far better than many others in this business. **PRISM**