Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

Remarks as prepared for delivery by James R. Clapper Director of National Intelligence
Defense Strategies Institute (DSI) Automated ISR Symposium

Wednesday, February 19, 2014
F Street Conference Center, Washington, D.C.

Thanks for that kind introduction, Tom [Engleman, Senior Partner, DSI]. Before I get into my remarks, I want to offer a shout-out to everyone at Defense Strategies Institute, for four reasons:

First, for hosting a conference designed to make a real difference to those trying to improve our national security capabilities.

Second, for your goal of being “a non-partisan, relevant, sustainable, and ethical organization.”

Third, for your exemplary internal leadership – which includes women, minorities, and veterans.

And fourth, for your outstanding work with the Wounded Warrior Project, which I think is especially appropriate, as we meet here on the anniversary of the beginning of the Battle of Iwo Jima, which to this day, is the only USMC battle in which American casualties exceeded those of the enemy.

You really are the “good guys” for helping our wounded veterans, and I wish there were more organizations like yours.

So, I understand that yesterday, you heard from the Director of our advanced R&D group, IARPA, Dr. Peter Highnam, about the work they're doing to advance the IC’s data analysis capabilities. And it sounds like this has been a great symposium, based on other feedback I’ve received.

My plan here this morning is to speak for a few minutes, following which, we can transition to more of a conversation. But first, let me provoke you.

As a career intelligence guy, I have never liked the term “Intelligence, Surveillance, and Reconnaissance” or “ISR,” ever since it was coined in the early nineties, when I served as the Director of the Defense Intelligence Agency.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

The reason for the term – and I was there, so I know – was to somehow de-limit what intelligence is and does, in favor of “operators” and “operations.”

I would simply ask you, why do you think we do “Surveillance” and “Reconnaissance”? We do it to gather intelligence. So for my part, the term “ISR” is a contrived misnomer, to marginalize intelligence. Let me know if I’m being too subtle here.

Of course now, this misnomer is an accepted part of our language. We all kinda know what “ISR” means; but I still have an aversion to it.

Second, a little history.

Now that I’ve achieved true geezerdom in intelligence – having done it for over 50 years in one capacity or another – I thought I’d share some historical perspective on the term “Automated,” as applied to “ISR.”

When I did my first tour in “my” war – Southeast Asia – I went to Vietnam in 1965. I was among the first 100 Air Force intelligence officers who went there PCS. Generally, “automated ISR” in those days was acetate, grease pencil, and two corporals.

One of my duties during the course of my tour was to be the “OXCART Control Officer.” OXCART was the project name for the SR-71, and it was a highly compartmented Special Access Program (or SAP), which flew missions over North Vietnam.

It was my job to hand-control every piece of correspondence having to do with the SR-71 that came to the then-2nd Air Division (later 7th Air Force), and then show these pieces of correspondence to a very select few generals.

It was actually a stressful job, since misplacing one of these documents could be a career-ender. It was all very spooky, and also mind-boggling at the time. This magnificent machine which could fly at unbelievable altitudes, and at unbelievable speeds, and was impervious to virtually all contemporary air defense systems.

The SR collected great volumes of ELINT and imagery – very quickly, comprehensively, and efficiently. The problem was that it would return to base at Kadena in Okinawa, and then some days later, I’d get message reporting on early mission results. By the time we got the actual imagery and ELINT read-outs, it was interesting, but not current – and thus of greatly decreased value.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

Let me fast forward to DESERT STORM. I served as the Chief of Air Force intelligence in the Pentagon. We had a marvelous overhead reconnaissance capability. The problem was that the primary mode of getting this imagery to the war-fighters in the AOR was by T-39 couriers. Again, good stuff, but not current.

So, we've come a long way since then, with the advent of our near real time overhead systems, and the revolutionary capabilities of our Remotely Piloted Vehicles, or RPVs (the term of art I prefer), and their unmatched capability to stare persistently, and to convey intelligence real-time, which accrues from the dramatic improvements in our real-time global communications capabilities.

This "ISR" capability has revolutionized intelligence. It's enabled the "find, fix, finish, analyze, and repeat" cycle that was first championed and instantiated by Stan McChrystal, (a personal hero of mine) when he commanded JSOC for five years.

That approach had spread to the conventional forces, and I would submit has had a profound impact on intelligence generally, over the last 13 years or so. All to say, the phrase "Automated ISR" has special meaning to me.

It wouldn't seem right if I didn't say something about the threat out there – just to remind everyone as to why ISR – automated ISR – is so profoundly important. So, accordingly, bear with me as I review with you what I've been saying to Congress during three open hearings over the last three weeks.

I also spoke about the impacts of the Snowden revelations. I won't go into that in these remarks. But we can certainly talk about it during the Q&A period, since there's a direct correlation between our capacity to address these threats, and the damage these revelations have caused.

A big part of my threat testimony opening statement was a laundry list of the crises and threats around the globe – and I have to tell you, looking back over my more than half a century in intelligence, I don't think we've ever faced more challenges. So here's what I just told Congress that we face today:

- The scourge and diversification of terrorism, loosely connected and globally dispersed – to

include here at home, as exemplified by the Boston Marathon bombing, the sectarian war in Syria, with its attraction as a growing center of radical extremism, and the potential threat this poses to the Homeland.

- The spill-over of the Syria conflict into neighboring Lebanon and Iraq.

- And, the destabilizing flood of refugees in Jordan, Turkey and Lebanon – now almost 2.5 million, a symptom of one of the largest humanitarian disasters in a decade.

- The implications of the drawdown in Afghanistan. This year is a cross-roads – with the drawdown of ISAF, the Presidential election, and whether the Bilateral Security Agreement is signed.

- The deteriorating internal security posture in Iraq, with AQI now in control of Fallujah, and violence across Iraq at very high levels.

- More than 5000 civilians were killed in 2013 – Iraq's deadliest year since 2007.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

- The growth of foreign cyber capabilities – nation-states, as well as non-nation states, to include fledgling cyber attack capabilities by certain terrorist groups.

- The proliferation of weapons of mass destruction.

- Aggressive nation-state intelligence efforts against us.

- An assertive Russia.

- A competitive China.

- A dangerous, unpredictable North Korea.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

- A challenging Iran, where the economic sanctions have had a profound impact on Iran's economy, and have contributed to the P5+1 Joint Plan of Action.

- Lingering ethnic divisions in the Balkans.

- Perpetual conflict and extremism in Africa – in Mali, Nigeria, CAR, South Sudan.

- Violent political struggles in – among others – Ukraine, Burma, Thailand, and Bangladesh.

- The specter of mass atrocities.

- The increasing stress of burgeoning populations – the world's population is projected to grow from 7.1 billion now … to 8.3 billion in 2030.

- The urgent demands for energy, water, and food.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

- The increasing sophistication of trans-national crime.

- The tragedy and magnitude of human trafficking – some 27 million people were trafficked last year.

- The insidious rot of synthetic drugs.

- Potential for pandemic disease occasioned by the growth of drug-resistant bacteria – 70% of known bacteria in the world have developed resistance to drugs.

I could go on with this litany, but suffice to say we live in a complex, dangerous world.

Obviously, the more help we get – from Congress, from partners (to include industry), from improved Science and Technology – the better off we are. And that's where automated ISR – among many other important improvements in the way we do business – comes in.

For the last part of my remarks, I want to spend some time on two "BIG IDEAS" that I think will revolutionize intelligence. In some ways, these two big ideas – IC ITE, or "Eyesight," and Activities Based Intelligence, or ABI for short – are very compatible with, and complementary to – the huge strides that have been made with RPVs.

First, IC ITE.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

IC ITE is about implementing our next generation of IT, using technologies that are already in use today in many of our agencies. We'll transition from individual agency-centric IT – and what I would charitably call a "confederation" – to a single architecture. This is something we've talked about for years, but just never had the incentive to actually do it.

I believe we've just about squeezed all we can out of the current IT Enterprise turnip, so we need to do something different. We're using these financially austere times as an opportunity to take integration to the next level. This was driven initially by money, given the huge and disproportionate share of the NIP budget that we spend on IT.

So, all the agencies are taking their big IT budgets, and working together to make sure we have (1) a cohesive architecture, and (2) a more uniform structure – that every agency understands, and can build to. That by itself will enable much better intel integration, my # 1 goal for the IC, by bringing data together in new ways, and by adding common strategy, services, and collaboration tools. It's going to aid integration, be more affordable, and be more secure.

The bumper sticker mantra is: "Tag the data, tag the people." Our Business Strategy will lay out how IC elements will order and pay for services provided by other IC organizations. This will operate very much like the commercial market – there will be service providers, and there will be consumers. And, the IC Components will be mutually dependent on each other for these services.

A major advantage of all this is that when fielded, we can substantially reduce the size of the marching Army of IT contractors, which I realize is not necessarily "good news" for everyone, but it is the right thing. Bear in mind, we started all this well before Snowden, but insider threats posed by people like Snowden serve to give this even greater impetus.

In the last two and half years, we've made very good progress. IC ITE went from a concept (an idea on a whiteboard in a conference room) to a unifying, community-wide strategy and series of implementation plans, developed by the agencies with our "light" oversight. We developed and agreed to a security framework.

Last August, we began basic early operations. We now have over 3500 common desktops at DIA and NGA. Agencies are sharing their applications in a new Applications Mall – which is similar to online apps stores where we download games for our kids, and mortgage calculators for us. We're moving different types of intelligence data into a government-developed Cloud – to test data integration and access controls, and make sure sensitive data is only accessible to people who have the right authorities.

Remarks of DNI Clapper at Defense Strategies Institute Automated ISR Symposium

CIA recently contracted with Amazon to bring successful commercial cloud services into our secure domain. And no, the IC's clouds are not on the internet.

How is it all split out, as far as responsibilities? We're leveraging the unique technical capabilities and experiences of IC agencies. CIA and NSA are leading the cloud development and the Identity Management and Authorization segment. NGA, with DIA as a partner, is developing common desktop service and leading Enterprise Management. NRO leads Network Requirements and Engineering to achieve efficiencies – and, I might add, is doing a fantastic job. NRO is approaching this with the same rigor they apply to getting ready for a launch.

We'll continue to evolve to this more modern and common IT infrastructure – in incremental steps – over the next several years. And for such a big activity, we've had to be cognizant of not only technical challenges, but cultural ones.

This really transcends IT – it's a significant change from the past. Operating as an Enterprise requires trust across agencies, involves change management, and adoption strategies.

Let me turn now, much more briefly, to the second "big idea" I want to talk about.

This one centers around the way we think about so-called "Multi-INT", or what we're calling Activity-Based Intelligence, which will be ultimately manifested in the future generation overhead architecture. The vision is to bring the disciplines of SIGINT and GEOINT together in the same time domain – more integrated and agile. It will enable us to look at activities in an area over time, to better forecast events, and quickly alert analysts to where the action actually is taking place – as opposed to trying to predict where it might be.

In other words, we'll be able to discover and track how our adversaries live, the activities they're engaged in, and the patterns of their lives, and manage our collection accordingly. We'll be able to automate change detection across our intelligence systems, based on user-defined algorithms, and recognition of events in videos and open source. This will lead to greater cross-INT, cross-domain, and cross-agency tipping and cueing of our collection, AUTOMATICALLY, whenever things or activities of interest are detected.

As far as innovations in ISR go, this probably has the most profound future. It's going to give analysts the figurative "joystick," and let the intelligence problems drive collection. It's really a sea change – a different overall attitude, and a much smarter way of doing business.

But it's important that we also consider all the implications of these innovations, and make sure

we have civil liberties and privacy protections in place. We need to be as transparent as possible, while still protecting sources and methods.

So, let me stop here and take some questions.

###