DANIEL MORGAN GRADUATE SCHOOL
of
NATIONAL SECURITY

presents

"Intelligence Challenges in a Volatile World"

David Shedd
Former Acting Director,
Defense Intelligence Agency

I hope that, in the course of what I have to say, you are thinking about questions or remarks or comments that you wish to make as I go through some topical issues that I think are informed by the past, but are yet to unfold in terms of our future. I am absolutely passionate about looking at the future; again, informed by our past, but not wedded to our past.

The key point is that our intelligence customers have a right to demand much from an intelligence community that, to the taxpayers, is somewhere in the order of 65 billion dollars, maybe approximating seventy billion dollars. You take two major lines of funding, one which comes from the National Intelligence Program, which is what under-writes the funding for the intelligence community of sixteen agencies, to include the office of the DNI, with its creation in the Intelligence Reform and Terrorism Prevention Act of 2004, but really stood up on its own in May 2005. And then the military intelligence program, which is really the stewardship for the Undersecretary for Intelligence in the Department of Defense. So when you combine that, it's approximately seventy billion dollars.

The challenges, however, are absolutely extraordinary in terms of what our nation faces. You can now pick up, for us old-timers, a newspaper, or look at the media, for those old timers and young people, in whatever form you get your news; and most recently, as we have seen in the course of events in Orlando, and as we look abroad, the instability that we see. The bottom line here is that our customers—the President, the Congress, the combatant commander, the chiefs of police of major cities—expect nothing less, but a performance by an intelligence community to deliver a currency, called intelligence information, that provides them options that create a decision advantage. That is, having knowledge of something that the adversary doesn't know that *you* know.

I will violate my own rule and offer two taglines instead of one for today that I hope you can take away from today's remarks.

Tagline number one comes in the form of a question; and we'll come full circle in terms of application to this question as we go through the rest of the presentation. The question is as follows: Are we already in,

This article is derived from remarks delivered at the Daniel Morgan Graduate School as part of the 2016 National Security Lecture Series on July 8, 2016.

or entering into, a technological exponential age? Where the rate of change of technology, for those who know Moore's law, is easily 2.0, if beyond now.

In 1998, not that long ago, Kodak had 170,000 employees and sold 85% of all photo paper worldwide, and went bankrupt as a business model in just a few years. Software will disrupt most traditional industries in the next 5 to 10 years, and I would say it's already occurring. Uber is software, but no cars are owned by Uber. Airbnb is now the biggest hotel company in the world, but does not own properties. Artificial intelligence; IBM's Watson provides 90% accuracy in basic legal advice; compared to 70% accuracy with human-provided legal advice. Think about that. Watson's diagnosis of cancer is four times more accurate than human diagnosis. That's artificial intelligence. And we're just at the tipping-point of where that aspect is going. SIRI, Watson, and versions that will continue to unfold. Autonomous vehicles will redefine car ownership, insurance, urban living, and so on. This is just but a small sampling to set the stage against which we have to view the world and how it applies to intelligence.

So tagline number two: Bureaucracies will choose failure over change, unless… and we'll talk about what comes to finish that sentence. The most obvious thing is of course leadership, risk taking, the ability to look at the past and be informed by it yet not live in the past as I said already. There has been a decisive shift from a dominant position for the public/government sector to the private sector.

As the examples that I gave, the public sector does not control either the type of technology innovation by and large, and much less the pace of it. So autonomous vehicles, artificial intelligence, genetic engineering and biotechnology, cyber, quantum computing, Internet of things, imagery resolution and revolution, drones, 3D and now 4D printing. See, we are in a world that was predominately, for many decades, a world in which that was developed -- in the research and development sense of the word—in the government space. And by extension, the pace of development was controlled by government, and therefore by extension the usage of it, and the purveying of that technology to customers outside of government space was controlled. You see, against that backdrop, bureaucracies will choose failure over change by saying we can still do it inside government.

Now, that isn't to say it can't do anything. There are the DARPAs and the IARPAs. They do some extraordinary things. But if you talk to the head of IARPA, which I've done recently with Jason Metheny, it is very clear that it is done in partnership with the private sector, with a preponderance of what they're actually doing, done with the private sector. So it's an IN-Q-TEL-like model called IARPA, in terms with where they are headed with big data and big data analysis and big data intelligence.

So let me turn a little bit to the diversity of the threats that we face, against which we and our friends and allies face enormous national security challenges. The globalization, I argue and maintain, of technology has democratized information and technology to the point that greater complexity, rather than less, exists by way of the challenges that we face in terms of the threats to our nation and to our friends and allies. Countries that used to be technologically back-ordered, or certainly technologically incapable, can now benefit from advanced technologies much faster, that are either similar or very close to the very top developed technologies of top-tier countries such as ourselves. All without having to make a serious research and development investment. Some steal it, others just buy it legally and openly. And because these countries can present a much higher threat than they used to, they effectively enter the tier one countries through technology. Sometimes and mostly through a front door, but many of them also through the backdoor.

This demands our higher prioritization and intel sources to track the countermeasures that come with those capabilities that nation states—and as we well know, that non-nation states—acquire. There is then a convergence; think about this as you think about the globe, of regional or functional technology threats that emerge from that. This is a different threat matrix than certainly the one of my early career, the 1980s and even into the 1990s, in terms of what a CIA mission consisted of. It is no longer sufficient to have an intel officer only with a regional expertise. That officer needs to be well versed in technical disciplines to be more productive, if not completely productive.

It presents a conundrum for you young people. Do you go the generalist route, or do you go the specialist? I would argue it's a hybrid. The private sector can certainly help shape that in terms of the investment that you make, in terms of your career development. And now the adversaries understand our reliance on technology for conducting military operations, and they seek to exploit that reliance and remove us from our own comfort zone, of believing that we have in fact control of that effort. Take the F-35 for example, the most advanced aircraft ever produced; it is at milestone decisions, which is just a fancy way to say setting goals and objectives at a certain point in its production. It is consistently a year or years behind already before the adversary is already adapting to aspects that the F-35 has. That's how quickly the world's changing, and that's how quickly our adversaries are adapting accordingly.

So this is obviously not a go around the world and tell you this is the threat in North Korea, versus Iran, versus Syria and Iraq and ISIL and Al-Qaeda, the Al-Nusra front, etc. I am happy to talk about those, but I'd much rather that you apply critical thinking against these threats, in this relatively new brave world that we're looking at.

The key point is that technology at a cost point is getting cheaper by the day; allow me some freedom in saying that. Obviously not every technological piece, but relatively speaking to where we were even a decade ago, things are much cheaper and the market entry is enabled by commercial R&D and applications and no longer principally under government control. That's the bottom line of this scene-setter.

Some additional points that I would like to underscore here: The access to technology used for military applications—and this is something that was drilled into me with my experience at DI—emboldens our adversaries in getting into a confrontation earlier and more deeply with us, as a result of feeling that they have parity *vis-à-vis* us.

Now, think of war in the grey. Think of the challenges, the challenges of confrontation opposed to World War Two *per se*, or the Vietnam War. Think of a less traditional model of what that confrontation looks like. And that statement that I just made would be absolutely true, that the likelihood of confrontation increases, as the level of a sense of confidence goes with it by way of what technology brings to our adversaries.

And in so doing, some of our adversaries, whether state or non-state actors, seek to challenge our American leadership in the world. I will not get into the US side of leadership or lack thereof; that's not the point here. Our adversaries will challenge it; that is in fact the point. Cyber enables these adversaries, by the stealing of intellectual property rights and [proprietary] technology. The adversaries don't have to spend any, or they spend very little, in R&D by simply stealing those property rights to reduce their time in the weaponization and other aspects of their capabilities in operationalizing them. So the asymmetric threat increases from adversaries due to this low price of entry, giving the intelligence community a much bigger challenge in detecting it; and then giving policy members of the policy community more options in terms of countering these threats.

And so, in the end, to sum up this commentary on the portion of technology: as the adversaries seek, from their perspective, to create a level playing field with the United States [and] our friends and allies, whether it be in their weapons capabilities or their intelligence underwriting or collection—those systems that they use. Regarding the impact of these emerging technologies, what is available to us is increasingly available to our adversaries. That is the main point. This change in technology landscape, actually levels the technological playing field between the US and our allies against our adversaries in a conflict. They do and intend to take what the intelligence community and the defense community calls COTS: Commercially OFF The Shelf capabilities, which is the technology that is readily available, and then they weaponized it.

Think of drones, think of the capabilities of 3D printing. Think creatively of what an adversary can do at a relatively low cost. And then those same adversaries can very readily proliferate that technology adaptation to other partners in their efforts to challenge the United States and our allies. Though the loose nature of many technologies makes it increasingly difficult to control, and yet another intelligence challenge in terms of detection, and then to stop that sharing of technology amongst the adversaries. Near-peer competitors by 2020, 2025, in certain areas of weaponization, like Russia and China, will proliferate dual-use technologies in order to enhance their revenue streams.

Let me give an example of where we are incredibly challenged. This comes more out of my DOD experience, by way of the Defense Intelligence Agency, than it does out of CIA. Although clearly, CIA would have an intelligence interest in both the collection and analysis of this. And it is in the area of anti-access aerial denial (A2AD). You hear those terms, and you young people will hear it a lot more; what it essentially does in its essence is deny US capabilities into the airspace, or water space of our adversaries. That is our ability to enter and challenge that adversary inside their airspace and out a certain percentage or certain area that they wish to protect outside of their immediate borders.

We see this in the application of Syria for example, through radar systems where the Syrians have been enabled through the Russians, to prevent us from going into certain spots of their airspace well beyond the confliction because of advanced radar and intelligence capabilities by Russia, which in this case is an adversary [which], in that immediate area, is preventing that. So Russia pursues technologies and strategies very actively in this area of anti-access aerial denial. So intelligence is proven critical. In the meantime, the signals that we would call telemetry that comes from all of that is encrypted, making it even more difficult in terms of the challenges to collect it and to decode it, in vernacular language.

Several technologies and weapons systems can be bundled and employed as a collective strategy, then, to prevent that access to that airspace or water space or land space. The A2AD type strategy, multi-layered and multi-pronged, is at the core of the Russian modernization program in the military. It is not only effective in preventing the effectiveness of US and allied systems, but more importantly it effects Washington's decision calculus when it comes to policy choices. Because what you've done [is], instead of working with an entire loaf of bread of options, you've already said "I can't do X" because that's already a forbidden zone. That, then, prevents certain options for the policy makers if you cannot penetrate that A2AD. So at points, you may very well make a policy decision that says we will not engage, or the cost of engaging is too high […] in order to go that direction.

So responses to the challenges that I've laid out that have been very heavily technology-driven. Are we ready? I would argue no. I think that there are very foundational things that have to dramatically change, that I don't want to get into today. But I'm a big believer that the acquisition processes—I've talked about the F-35 system—is woefully broken. It is simply not working to our advantage. It's too slow. It's generally too late in terms of how you get into it. It doesn't reward innovation by the big thinkers, but by the small producers to get into that stream of acquisition, and so on and so forth. As a rule, I have found that in the 18 months that I've been out, and the companies that I'm dealing with, is that commercially off the shelf capability is good enough in many instances, I would argue in the vast majority of instances.

For example: If I am in a counterterrorism environment analytically, or even operationally, it is probably a good idea that I not look like a terrorist. It's just a guess. You students don't go into the deep dark web and look like them; the FBI will come a-knocking. I'm quite sure of that. So what do you do? You manage your attribution; you manage your persona in such a way that your ISP is not tied to you. It seems very logical. I won't promote a certain company that does this, but there is company that does it very well, a former agency CO leads it, it is able to do marvelous things that hide your ISP. I do a fair amount of travel overseas; I never get on the web using David R. Shedd. When I go to my web browser, which is this alternate universe, there's no latency to it at all, it randomly chooses out of thousands of ISPs out there. Then I can go do a search on the name of a person, or whatever it might be. I want to hide that attribution. Why would government on God's green Earth try and develop that itself. That makes no sense. It needs patches all the time, it needs IOS 10.0, so let the companies do that, deliver that as a service. Some of that is occurring, but a lot more of that has to occur. But remember, bureaucracies will choose failure over change, unless there is leadership to drive it there.

The future challenges, and opportunities, are indeed enormous. And it is rapidly changing, and is revolutionary. Back to question I asked, this Tagline #1. Is it truly revolutionary? I truly believe it is. By the way, when I say technology is changing, that does not necessarily mean everywhere. It's interesting, airplanes don't go that much faster than they did twenty years ago. They still fly around at about five hundred and fifty miles an hour at thirty-nine thousand feet, depending on which direction you're flying. So it's not everywhere. But certainly in the area of communications, in data handling, and data processing and all that, it's revolutionary.

What can we do? Let me give you in closing seven ideas for action—and by no means are these intended to be inclusive to every possible idea to do. But there are somethings that I have thought about and continue to believe would be of high value against the backdrop of what I have described.

Number 1: I think we have to dramatically increase the public/private industry collaboration. There are enormous challenges in this post-Snowden environment to do that. Do not let me leave you with the impression that something is easy to do. But nonetheless, it is imperative to do. By that I mean it is no longer a choice, but a matter of survivability. Because of the dramatic shift that has occurred over the last decade, decade and a half, to two decades, at an increasing rate of speed in terms of where innovation is occurring on the edge. We need to be doing that with the private sector. Solutions are far more prevalent there, and then the absorption, where that bureaucracy that chooses failure over change, has leadership that drives it to that.

Secondly: The talent acquisition could be modified with hiring practices where the public sector has far more of a rotation in the private sector, and vice versa. It is a different HR model entirely to what we have now. Essentially you have a career, command, and then retire. It is less so now than when I came in, but you are seeing an intelligence community for you young people who are looking into potentially, a career inside the intelligence community, or the defense Title Ten area of defense intelligence, of very much almost a disloyalty if you leave. Because you were invited into the club, you joined the club, but now you just, what is it, American Express card when you leave? So one of the things I did at DIA was keep the active clearance for seven years to anyone that left. It was low cost, and the probability of a good number of them returning back to somewhere in the intelligence community, not necessarily DIA, was pretty high. Because, if you go to the very core, the motivation is these individuals have a passion to serve and make a difference. The grass may be greener for a while, and that may not be bad by the way, on the outside, but you'll come back. Or a good percentage will come back into service in the government. It is an incredibly, incredibly rewarding career. So if I were to do it all over again, I wish I would've known, even things I've learned over the past eighteen months, much sooner. Just by way of the experience.

Third: Obviously government employees would have to be interviewed and selected by the industry, but would be invited into industry to spend time there, and it would count for joint duty. If you take the Goldwater-Nichols version inside the Department of Defense, which really highlighted this cross service—as in the uniformed services having these experiences—I think the civilian side ought to give credit for that one year, two year of where you go to Silicon Valley and come back in, maintaining your security clearance during that time. I think that will encourage greater out of the box thinking in government.

Government cannot possibly own all of the expertise that the private sector is continually producing. And for that I would argue, what we really need is a national brain trust, if you will. A reserve that you could tap into for individuals who have that private sector experience, and don't come in with all the government constraints of a GS schedule. Some of that is done, but it is miniscule today and needs to be increased significantly. The Steve Jobs, Jeff Bezos, and others to come in and do that. How attractive that would be—if it's done the way government does things, it's not really that attractive. I understand that. So you have to change the modalities under which it's done.

Five: We talk a lot about this. I still think government tends to stifle unconventional thinking rather than reward it. The thinking that really is out on the edge on how to deal with these critical issues that I've described.

Six: Cyber is our single biggest challenge. For those who are sitting toward the back, as you think about how you're going to be attractive—I know you're attracted, but being attractive to the ones that would hire you—cyber is going to be an integral demand for years if not decades to come. That is, your ability to play in that space, understand that space, counterintelligence in that space of cyber, is going to be critical. Allies and friends need to come together much closer in areas of combating the cyber threats that we face. I am a big advocate of taking [it] out of hiding inside the intelligence community today, and creating a NCTC for cyber. I know there's a small one, capped at fifty and all that; it's not enough. The threat is far bigger and far larger and deeper in the cyber arena. And again, it would tie into this public/private sector partnership.

Lastly: foreign partnerships. It is time to significantly and dramatically increase our dependency and shared responsibilities to counter threats. I would start with NATO and the twenty-eight countries there. I would revisit the Japanese and South Korean agreements. Not as in devolving them or countering them, but rather building them much stronger in the region. I would invest heavily on India, and places around the globe. You can think yourself, but the partnerships are absolutely against the common threats which are growing. That is not at the expense of unilateral human intelligence, unilateral signals intelligence, or even unilateral cyber collection. But the partnerships are absolutely critical in terms of the response.

In conclusion, the national security, and by extension the intelligence demands are indeed enormous. Many of you are part of that future. But it is not, by any means, insurmountable to come out on top over the adversaries.