LexisNexis Open Source Intelligence Roundtable
"OSINT 2020: The Future of Open Source Intelligence"

Keynote Address:
- **Dan Butler, Assistant Deputy Director for Open Source, ODNI**

Panelists:
- **Alex Joel, Civil Liberties Protection Officer, ODNI**
- **Doug Magoffin, Chief, Defense Intelligence Open Source Program Office**
- **Kevin O'Connell, Adjunct Professor, Georgetown University**
- **Mark Gabriele, Associate, Booz Allen Hamilton**
- **Kenneth Rapuano, Director, Advanced Systems/Policy, Mitre Corporation**

The National Press Club
Washington, DC

June 17, 2010

Video of this event is available online at www.dni.gov/video.

The LexisNexis-hosted OSINT Roundtable was created to make a public space for discussion about the government's needs for Open Source Intelligence—a recognized discipline in strategic and tactical national security decision-making—in order to facilitate relationships between government officials and private sector leaders.

ANDREW BORENE: Good afternoon, everybody. Welcome to the first Open Source Intelligence, or OSINT, Roundtable at the National Press Club. My name is Andrew Borene. I'm a program manager with LexisNexis, and I want to thank all of you for joining us.

Earlier, before the start, we were looking down the list of attendees with some of the panel members, and I have to be honest; I wanted to make it a point to recognize some of the VIPs in the room but there are actually just too many and I would screw it up and violate protocol – and I'm a former Marine lieutenant and I might cry in front of all of you if I tried that – (laughter) – so I don't want to do that. But I do want to thank you all for being here. It's really an impressive audience and an amazing collection of leaders from the government and the private sector.

And that's really what we're hoping to do with this event was – this was a brainchild that kind of spawned from some conversations I'd had with people in the private sector and in government that work in the open source intelligence area as a discipline, and that it is an area that may not have a

set program sponsorship at the federal level; however, there are needs from the government and we need to collaborate and find solutions that answer those needs.

So hopefully, as you were waiting here, some of you had conversations about that, and certainly afterwards, after this expert panel talks, it will set a tone for some continued conversations that lead to innovation that meet the needs of our national security professionals. And that's really the goal here, to facilitate relationships and create an increasingly responsive open source intelligence infrastructure for the government.

And before I introduce our panelists, I just want to make special mention and reference to the Americans that serve in our armed forces and our law enforcement community and in our intelligence community.

I worked for a Marine major once who reminded me that intelligence is a customer service line of work, and who that customer is is the warfighter at the front line, it's the cop on the beat, it is – in this line of work at times it's supporting people who do not get recognized for taking amazing risks on our behalf, so I just want to express our thanks for that service. They're not with us today but we're thinking of them.

And what I'd like to do now is introduce our keynote speaker and our panelists. Our keynote speaker is the assistant deputy Director of National Intelligence for open source, Mr. Dan Butler. Our panelists come from across the spectrum of the private sector and government with an amazing – really, if you look through the bios in your package, the level of experience in this group is mind-blowing.

We have Dr. Gabriele from Booz Allen; Mr. Doug Magoffin, the chief of defense intelligence, Open Source Programs Office; Mr. Rapuano from MITRE Corporation, with very extensive senior government experience; Mr. Alex Joel, who is the civil liberties protection officer at Office of the Director of National Intelligence; and Mr. Kevin O'Connell, professor at Georgetown and CEO and president of Innovative Analytics and Training.

And amongst this group of experts, Mr. Butler is going to set the tone talking about a vision or an idea for what open source intelligence may look like in the year 2020 and, a decade from now, what are those needs that the government has, or what are the things that we can do as private sector and government persons interested in meeting those needs – enhancing the security of our country and enhancing the competitive advantage for our nation.

So that is the theme. I would like to introduce our keynote speaker, Mr. Dan Butler. Mr. Butler has been the assistant deputy Director of National Intelligence for open source since 2008. Previous to that he was at the Office of the Director of National Intelligence since 2006 and has over 24 years of experience in the Department of Defense intelligence community.

I read his bio. He has handled the TARPS Aerial Reconnaissance Pods. He has handled human intelligence or human collections requirements. He has handled congressional affairs on the Hill with experience at NCIS. There is famous television show about that, sir. I don't know if you're aware of that.

DAN BUTLER: It's my favorite show. (Laughter.)

MR. BORENE: And he was also the executive director of the Air Force Office of Special Investigations, which I don't believe there is a famous television show about that one –

MR. BUTLER: Not yet.

MR. BORENE: – but perhaps there will be some day. But we are very, very fortunate to have such an amazingly distinguished panel. And after this I'm going to step out of the way and let them kind of manage the show.

Each of our panelists will talk briefly about their experience and vision and then we'll open it up to audience questions. And with that I would like to introduce our keynote speaker, Mr. Dan Butler. (Applause.)

MR. BUTLER: Thanks, Andrew. Actually, I would like to thank Andrew and LexisNexis and the National Press Club for hosting this event and doing the difficult work of organizing it.

When Andrew suggested this a couple of months ago now, I think it was, he told me there was a hunger for discussion in our community, in our professional community, about open source intelligence, and he reminded me of the conference we had – three-day conference back in 2008. And I thought, yeah, there might be a hunger for it, and I was surprised actually when I saw that he had to cut off registration for the event today.

And I appreciate the great turnout, and it's kind of like a reunion. I'm seeing a lot of really terrific people, people that were pioneers in this business, people like Peggy Lyons (sp), who actually wrote the first Intelligence Community Directive 301 on the National Open Source Enterprise; Dr. Dick Ward from the University of New Haven, who is truly a pioneer in the academic community in terms of bringing open source exploitation capability to the forefront. And I saw that firsthand when he was the dean at Sam Houston University. So really, this is a pleasure for me to be able to see so many good friends and colleagues.

I want to thank my panelists, my colleagues, who have taken time out of a very busy schedule to join us here today. Alex Joel is jumping on a plane as soon as we finish up here and going off to speak somewhere else. Ken Rapuano came rushing up 95 to be here to join us today. Doug Magoffin was probably just lingering in the hallway somewhere most of the morning. (Laughter.)

DOUG MAGOFFIN: Watching soap operas.

MR. BUTLER: But we really were fortunate to get people like Kevin O'Connell and Mark Gabriele, who can tell us a lot about what we should be anticipating in the future for open source intelligence.

And I want to thank all of you for coming. I know you all are very busy, and I know from knowing many of you that you are critical to the overall enterprise, what I consider not the intelligence

community but the community of intelligence that we in the IC need to tap into to be able to do our job most effectively.

Let me start by just saying that – telling you a little bit about my small office. Peggy has heard this a few times. My small office was established by our first director of National Intelligence, Ambassador John Negroponte during the first year of the ODNI, and we were charged with advocacy, integration, evaluation, oversight and guiding strategic investment in our National Open Source Enterprise.

And I'm reading this to you out of the first Intelligence Community Directive 300, that actually outlined responsibilities within the DNI, within the Directorate of Collection, for various disciplines that we needed to provide oversight for for the entire community.

Now, I'm also charged with encouraging community collaboration, building public-private partnerships, overseeing the DNI Open Source Center and two other national centers. In my advocacy role, I'm a big believer in public discourse about our profession, within the bounds of discretion of course, and believe we have a responsibility to think strategically about our future intelligence community enterprise.

I'm proud of the dedicated men and women who have built and sustained our nation's open source exploitation capabilities. They are extraordinary professionals. They include librarians like Janet Burke (sp), who is sitting here on the second row, the librarian up at the National Air and Space Intelligence Center. I've watched Janet play a leading role in building our National Open Source Enterprise for the intelligence community.

Events like this one allow us to contemplate how the future open source environment might present us with new challenges and new opportunities – opportunities to do our job better, more efficiently, and honoring our pledge to safeguard our national security and protect and defend our Constitution and our values.

My job this afternoon is to provide some foundation and some context for you and the exceptional panelists that have joined us today. We're here to think towards the future, 10 years hence. Now, I've always found that it's good, if we're going to have a panel and discuss something like OSINT, that we should define right from the outset what we're talking about. So let me offer to you the official definition of OSINT, at least the official IC definition.

"Open source intelligence is intelligence produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." That comes from the Intelligence Community Directive 301 entitled "National Open Source Enterprise." And we didn't make it up. It was cribbed, actually, from law – the National Defense Authorization Act for FY 2006.

"Open sources" is kind of a term that's in vogue. I would say it's in vogue today because we were trying to think of a better way to capture what we're doing today as opposed to what we've done for decades, because really we're not doing anything much different than we did during World War II or during the Cold War.

Open source is research. It's good research. It's rigorous and disciplined research. And I could give you a lot of good examples of how our intelligence community back in the 1940s and 1950s was built on a very solid foundation of what today we call open source intelligence, or open source exploitation. Back then we called it research. We went to librarians to get us the information and to help us find the answers we needed in order to perform our job.

What I would rather do is focus in on the game changer. The game changer was the Internet. We are in the Internet age. Today, in 2010, we're grappling with a capability that is a tremendous force for good, as we have all experienced, I'm sure, and it can be used against us. It can be used against our national security. It can be used against our families. So it's a typical double-edged sword, a tool that can be used for good or for evil, and it's a tool that we have to figure out how to exploit best. The Internet has transformed the open source universe.

So what's the ODNI interest in open source exploitation today and looking toward the future? Well, I would like to talk about our imperatives. I think it's important to look back at, even just five years later, why we are here, or why I'm here at least and why my panelists are engaged in this effort with us in trying to develop a federated National Open Source Enterprise.

The Intelligence Reform and Terrorism Prevention Act of 2004, in Section 1052, states that, "It is the sense of Congress that open source intelligence is a valuable source that must be integrated into the intelligence cycle to ensure that United States policymakers are fully and completely informed. The DNI shall ensure that the intelligence community makes efficient and effective use of open source information and analysis." That charge doesn't come much more directly or strongly, I think, than was provided by Congress and that sense of Congress.

The WMD Commission reported out in 2005 in the wake of the 9/11 disaster, and they looked at open source. And one of the things that they gave and provided to us as our mandate, as our charge and as our imperative was that we needed to do more with open source.

The WMD Commission stated, "Increasingly, intelligence community professionals need to quickly assimilate social, economic and cultural information about a country, information often detailed in open sources."

Executive Order 12333 as amended states, "All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. All means consistent with applicable federal law in this order and with full consideration of the rights of United States persons shall be used to obtain reliable intelligence information to protect the United States and its interests.

"Special emphasis shall be given to the production of timely, accurate and insightful reports responsive to decision-makers in the executive branch that draw upon all appropriate sources of information, including open source information."

So these are our imperatives today. We're charged with ensuring that we make the best use of a vast and growing repository of open sources, and the Internet has dramatically changed the availability of open sources to the intelligence community.

Looking to the future – that's what we're here to do today. We want to try to look forward 10 years into 2020 and try to figure out, try to grapple with and deliberate on, what might the open source universe look like in 10 years and what might we, as the intelligence community, need to be thinking about? How might we partner with our important partners in the private sector, in academia, foreign partners?

The WMD Commission actually projected ahead what they expected to see if we as an intelligence community did our job and did it well. According to the WMD Commission, it is our hope that open source will become an integral part of all intelligence activities.

The WMD Commission also referred to a finding and a recommendation where they recommended that about 50 open source analysts – they called them "evange-analysts" (sp) – be dedicated to the task of going out into the intelligence community and spreading the gospel, so to speak, of open source and the power of open source.

But the WMD Commission wasn't thinking in static terms. The WMD Commission said, however, we have an expectation. "We expect that the need for these specialized analysts will not be permanent. Over time, the knowledge this group has about open sources is likely to be absorbed by the general population of analysts as a result both of their education outreach efforts and of the influx of younger, more technologically savvy analysts. As this happens, these open source specialists can be absorbed into the broader analytic corps."

Now, it's important to understand this charge or this expectation from the WMD Commission. For those of us in this business who are responsible for ensuring that the IC makes appropriate and best use of open sources, we have been tasked by the Weapons of Mass Destruction Commission essentially with putting ourselves out of business – out of the business of establishing, nurturing, governing an industrial area capability for delivering open source-derived intelligence to decision-makers. The WMD Commission's underlying message is that open source exploitation skills should be a core competency of every intelligence professional.

If we do our job well, we should see the U.S. intelligence community in 2020 exploiting, in a disciplined, ubiquitous fashion, the vast, pervasive and persistent cloud of open sources of information that the Internet and other technologies are now making accessible and conceivable. Our efficient and robust just-in-time access to expertise, knowledge and open source-derived wisdom should improve to the point that we can truly focus more acutely on the most difficult intelligence challenges facing our nation using other means, more expensive means, more esoteric, other-than-open-source means of collection.

I think there are several factors that we need to think about as we look to 2020. The first is obviously going to be technology. We have already seen that the Internet is a game-changer and we are going to see, riding on the backbone of the Internet, more game-changers, and I think Mark Gabriele will talk – or speculate about what some of those game-changers might look like.

Smartphones. It's astonishing today what a smartphone is capable of and what that provides to anybody with access to a smartphone, and what it provides to people that can get that material that people that have a smartphone can access.

GPS devices. Some of you, like my wife and I today, probably used a GPS device to get here. The GPS device in our vehicle – the Garmin, the Magellan, the TomTom – that is a tool that's empowered by open source data, NAVTEQ data, and that's a great example of the blending of technology and open source data in an interface that provides very actionable, timely, instantaneous intelligence.

Dr. Mark Gabriele will offer some insights into what we could be facing in the next 10 years and what those open source intelligence technologies could mean to our national security.

The second item I think we need to talk about are resources and risk. We should anticipate that our ability as a nation to fund ever-increasing growth in intelligence community budgets will end. What might that mean to our intelligence community, to our effort to exploit open sources? What about the relative capabilities of our adversaries? How might actual risk and the U.S. public's tolerance of risk change in the ensuing 10 years?

Ironically, despite our immense national wealth and unprecedented investment in intelligence community capability, one could argue that our comparative advantage as an intelligence powerhouse has eroded in recent years with the advent of the Internet and the astonishing access to data it affords to everyone – to your children, to our adversaries. The poor man's intelligence community is now available to anyone with access to an Internet café or a smartphone.

Our relative expertise and ability to exploit open sources is one advantage we would be well-advised to ensure we never cede to our adversaries. We must stay at the forefront of open source exploitation, innovation and sophistication.

What if budgets do fall? It's a trite but powerful aphorism that necessity is the mother of invention. My team recently examined what the future could look like if we were forced to deal with drastic budget reductions in the intelligence community.

We took an extreme case and simulated a much smaller nation. We used an actual nation, that I hesitate to name, with a much smaller intelligence budget to postulate and assess how the U.S. intelligence community might actually end up relying more on inexpensive, virtually free open source information to address many of our intelligence requirements.

Panelists today with extensive experience dealing with outsized challenges and constrained resources are two former Marines, Doug Magoffin and Ken Rapuano, can address how falling resources, changes to our comparative advantage over adversaries, our adversaries' growing sophistication and access to open source intelligence, and U.S. society's tolerance of risk and intrusion into our privacy can affect how we might use or might refrain from using open source technologies in the future.

Third, civil liberties and privacy – key issues that we need to think about in the next 10 years. Foreseeable and unforeseen advances in technology, fluctuating resources and adjusting comparative advantages enjoyed by our adversaries will have significant ramifications for our society, for our security, for our civil liberties and for our privacy.

Again, Ken Rapuano, enjoying the perspective of somebody with direct and intense involvement in our homeland security policymaking after September 11th, 2001, can discuss the tensions in delicate and shifting policymaking and political balance we must find between security and privacy. And he can speak to how that balance changes with events, the actions of our adversaries, and other factors beyond our control.

Our community's leading expert on civil liberties and privacy and what we as intelligence professionals must consider as we try to carry out our responsibilities is our statutory ODNI civil liberties protection officer, Mr. Alex Joel. Mr. Joel can speak to potential impact of pervasive Internet access to information about U.S. persons and how we must consider how and when we can, should, or should not exploit new technologies.

Finally, a fourth issue that I think we have to grapple with is how we organize and prioritize today to make most efficient use of open sources in the next 10 years. In my view, this is our real challenge. It's something we as U.S. intelligence professionals, intelligence community leaders, U.S. industry and potential partners, partners in academia, must collectively tackle.

If we aspire to make disciplined, rigorous and sophisticated use of open source exploitation; if we intend to make that a core competency of every intelligence community professional, what might that require? How will dramatic technological shifts affect our ability to get to that stage? Will our national demographics, as the WMD Commission suggest, help us achieve our goals, or will we need to do more to exploit our demographic advantages? Do we, in fact, enjoy relative demographic advantage or will other nations enjoy those comparative advantages and outstrip us in sophisticated use of the Internet as an intelligence engine?

With growing access to open source data and new tools and applications that can sift and mash up that data for relevance and timely action, how much, if any, of the open source intelligence exploitation industry will be the exclusive province of the U.S. government, and how much will we be borrowing or buying just-in-time, and possibly at dramatically lower costs, over the next decade? Mr. Kevin O'Connell and our entire panel can help us delve into aspects of these and other key questions as we contemplate OSINT in the year 2020.

Thank you for joining us today. I look forward to your questions, your insights and a constructive dialogue on these issues. And with that, I'll turn it over to you, Andrew.

MR. BORENE: Thank you, sir. Our next speaker is Dr. Gabriele from Booz Allen, who will be speaking about technology and future implementation.

MARK GABRIELE: I'm just waiting for my slides to come up, but I was delighted to be invited to speak today, and part of the reason was when I was told the subject matter being the future of open

source in the year 2020 and I was asked to speak about technology I said, oh, good, I get to make stuff up. So you can't pin me down on anything.

Could you slide that this way a bit so I can see it? Thank you.

So having said that, you can't hold me to anything I'm about to say except the stuff that has already happened, so let's go.

I decided to look at kind of a particular case of technology adoption and use that as a basic model, so I looked at Africa. Now, everybody starts by looking at the past to try to predict the future and do the extrapolation. Well, in the year 2000 in Africa there was about 2 percent of the population that had cellular telephones. That's changed bit. If we look today, it's nearly 33 percent of the population, and actually that's kind of low because the population demographic in Africa skews young.

So if you think about adults carrying cell phones, it's actually closer to half or more adults carry cell phones, and that's throughout the continent on an average basis. If you look at North Africa, the penetration is in the mid-60s, and if you look at certain countries like South Africa, for example, the penetration is nearly 100 percent. Everybody has got a cell phone.

So what's telecom technology look like in Africa? Well, what did it look like in the year 2000? It looked like just about nothing. Now, this is what cellular technology looks like in Africa today. That is a common phone in Africa. That is a Motorola Timeport, and it's got a catchy name of L3089, I think – one of those things that sticks with you.

That was introduced in the year 2000, and that phone has – one of the big features that they advertised was you could set it to vibrate. That's what cellular technology looked like in our country 10 years ago and that's what it looks like largely in Africa today. It doesn't have a Web browser. You can send text messages with it. It is a multi-band phone so it can roam to other different networks, and that's very important. Next.

Now, like I said, it's a pretty capable little unit. It does what you expect a basic cell phone to do. It did for me. I owned one of these things 10 years ago, but like I said, if we're talking about the African continent, that's pretty much what people carry; small Nokia phones with similar feature sets, that phone, that kind of thing.

So what is telecom technology going to look like 10 years from now in Africa? Go ahead. I'm guessing it looks a lot like this, which is what we are carrying today. That's a picture of an iPhone 4. Now, it does a little bit more than just have multiple bands and the ability to send SMS messages. It has a full 30-frame-per-second high-definition video capability. That's 720p video. It has a five megapixel camera.

It has a GPS. In addition to the GPS it as a compass, it has an accelerometer and it has a gyroscope, which means if I decide to take a picture with that camera or take a video with that camera, the camera can tell me not only where I was standing but where the phone was in space. It can say, you were looking in the direction of 130 degrees and you held the phone at an angle of three degrees out

of vertical, and you were moving the phone too while you took this video, so you panned to the left at this speed. I can tell you exactly where that phone was when it collected that image or that video.

It also has the – like I said, it's got the GPS so you can just flip the phone on and leave a trail of breadcrumbs. It can serve as a tracking beacon. It can serve as a location device. It can do all kinds of things. And it has way more computational power than the computer you had on your desktop a few years ago, and that's all internal to the phone. And, oh, yeah, it's got better battery life than the Motorola I just showed you. Next.

Visualization tools. Again, I looked at the past and tried to project forward a bit. So the first thing is Google Earth. That came out several years ago and it's a helpful tool for visualization of all kinds of things. And if you'll click the link.

This is from a website called North Korea Watch, and it's pretty dense; I didn't extract out any of the points. But those were all kind of interesting places in North Korea, and how that map was populated was North Korea Watch said, hey, anybody gone to North Korea? You seen anything interesting? Make a note of where it is; sent it to us. And so people have and that's what it looks like. There's a map with all kinds of different bases.

And if you go to Google Earth and scroll around and click on those links, you'll find, oh, yeah, that's an SA-3 site. Isn't that cool? Because just people volunteered that data and it's been populated and collected over time. It's relatively static but it's there. And it's helpful and it's a useful way of visualizing and sharing information on a completely open source basis.

Now, move forward in time a bit. There is an interesting tool called Ushahidi, which is the Swahili word for witness. And it's been funded by a number of fairly reputable funding agencies – MacArthur Foundation, a lot of different people – Carnegie Endowment, I think.

What it does – if you go to the link – it was designed in the aftermath of the Kenya unrest in the wake of their elections in 2008 and the idea is that you set up a fairly lightweight little webserver and people can send text messages to it, they can send e-mails to it. They send whatever, just reports of stuff going on. It geolocates those things. It makes them available to everybody. It can send out a steady stream of messages. It can make them available on a map for you to look at.

It can do all kinds of stuff. It's been used recently in the aftermath of the Chilean earthquake. It's been used recently in Haiti, in the aftermath of that earthquake. And, actually, if you scroll down a bit there, there's a Sudan vote monitor listed at the bottom.

If you scroll down a bit further, one of the natural disasters they respond to is "Snowmageddon," the cleanup for Washington, D.C. (Laughter.) And you can go to that and you can click on it and you'll find people whose driveways need to be shoveled. There is a person here whose driveway is not shoveled. Or my street is blocked. People used it for that.

It's very easy to set up, it's very easy to keep operating, and it's useful. It's a better way to visualize information. And, again, how people interact with this can be anything but it was

designed to be really easy so it's – SMS messages; you can just text a little note to it with the geolocation of your phone, it will tag it, set it up, map it.

The next thing – if we can go back to the slide. There is a thing called Photosynth. This was an academic project that was actually bought up by Microsoft labs, and there is a website for it, Photosynth.net, and we're going to hope that our little demonstration here works because Internet connectivity is a little sketchy.

This is a panorama of photos from the Eiffel Tower. So somebody went up the Eiffel Tower and just stood there and took pictures walking around the periphery of the Eiffel Tower, and it's a view of Paris from every different direction.

Now, the tool recognizes similarities between the photographs and overlaps them, and if you see little different frames light up as the cursor moves around, those are each different photographs, and you'll notice that the angles are completely different. The software understands what the angle is, it warps the frame appropriately, maps it and uses it to build this wonderful mosaic picture.

And if you zoom in to any of those, you can zoom into the full resolution of the photograph. Now, these pictures – this particular example, these are all pictures that were taken at the same time. They don't have to be. As long as there is enough similarity in the scene for the software to recognize this is equivalent to that, and a couple of other parameters which are pretty simple are met, it will be able to map those pictures and identify them.

So there are cases of people going out on Flickr and other photo collection websites and saying, well, let me see about, oh, Notre Dame Cathedral and they'll collect thousands of images from across the Web of the Notre Dame Cathedral. And things that will get pulled in are if there is a picture of somebody standing in their dorm room and there is a picture on the wall of Notre Dame Cathedral, and that will get sucked in and it will get added to the mosaic.

The thing is really, really good at finding, identifying, tracking and logging in on these shapes. So this is relatively current. This is a couple of years old that this was introduced and it's still a thing that they work on. You can go to the website and play with it. It's very cute. You can add your own photos and synth up whatever you would like. Next.

So where do we go from here? Well, I started scratching my head and thinking about where – what's the logical next step in this technology? And if you go scroll that in. It's pretty straightforward to think about going from something like Photosynth to something like videosynth. If everybody has got a high-definition video camera in their pocket, you can take images from wherever.

Now, the fact that you know, exactly where the camera is, exactly what time it was taken – oh, by the way, to the millisecond because it's getting its clock time from GPS, so it knows exactly, where, exactly when, exactly how the camera was pointing. Given that information, heck, you can figure out the angle of the sun and you can get everything you need out of that information and you can construct – from multiple, different, completely unrelated observers in a crowd, you can get synthetic three-dimensional video.

So if there's any kind of event and anybody wants to, you know, go and take movies at, oh, yeah, there's going to be a protest rally, or there's going to be a pro-government rally, or there's going to be a whatever, if two or more people are there with their little camera phones, you can have a complete historic record, three-dimensional video – oh, by the way, because there's multiple audio streams, you can do all kinds of interesting filtering and pull out stuff from the background, pull out stuff from the foreground. You can do amazing processing.

And I'm talking about what we can do in terms of processing today. I'm not talking about – god knows what the processing capability is going to be 10 years from now. If you apply Moore's Law and the usual factors it will be pretty impressive. But that's just one application and that's just, you know, me on the back of an envelope in the course of an afternoon coming up with this.

So my takeaway message from all of this: In the future there is going to be way more information than any of us know what to do with, and if you want to try to avoid being drowned by this torrent of information, you'd better get started building the ark now.

And the way that I would recommend constructing that ark is paying careful attention to analytic technologies and analytic assistive technologies, putting together methods to catalogue the data, track the data, process the data as it comes in, recognizing that in future years you're going to be getting more and more of it and you're going to want to start gluing it together because not only can I build a synthetic image or synthetic video from images that were taken today, but I can use images that were taken last week, last month, last year.

So as I begin to build files of this interesting information, I can keep it handy, I can refer back to it, and I can keep taking new information in, pounding it against the old information that I have and seeing what new insights are revealed to me. And that's, like I said, just one thing that the future might have in store for us, and I'll be happy to come back in 10 years and have you all correct me. Thank you. (Applause.)

MR. BORENE: Thank you very much, Dr. Gabriele. Our next speaker is Mr. Doug Magoffin, the chief of defense intelligence open source programs.

MR. MAGOFFIN: A very hard act to follow. And just so you know, I'm suppressing an overwhelming need to karaoke here with this thing – (laughter) – right there. I've only been drinking coffee, so we're fine.

Well, good afternoon. I'm very pleased to be here today participating in this august panel, and in the process hopefully providing some interesting commentary on open source in the future. Although I've only been in my position a couple of months I'm not a stranger necessarily to open source or to the Department of Defense, and in fact I spent the last – the better part of the last 26 years working in support of defense missions worldwide.

My first exposure to OSINT was in the mid-1990s while I was serving as a military science and technology analyst. And in that capacity I relied almost exclusively on unclassified information that resided in the public domain to carry out my duties. Since then, I've gone on to serve as a

consumer, once again, of open-source information; most recently, though, as a coordinator of collection, dissemination and the like.

Since the focus of this panel is the future of open source, I'm going to limit my comments to what open source might be, what it could be 10 years hence. I'll base my comments on personal experience and observations accrued over the last 26 years, inasmuch as I won't be speaking on behalf of the Department of Defense or the U.S. government, which I'm sure they're greatly relieved.

I was asked by Andrew and Dan to briefly address the potential capabilities of those nations or nonstate actors that wish to do the United States harm. And to be quite honest, this is a pretty easy assignment. I don't have to cite any specifics. I don't have to provide any illustrative vignettes to make my point.

Really, anyone in this room that's worked open source and, quite frankly, has watched the evening news, surfed the Net or read a newspaper has gained an appreciation for the capabilities that nefarious characters around the world possess and those which they hope to possess in the future. You rest assured, if we plan on using open-source information to shape and understand the future operational environments, there's no doubt that the bad guys are doing the same thing. It just stands to reason.

So bearing that in mind as we move towards 2020 and we embrace technology and harness those capabilities that technology offers, we should also be willing to identify the vulnerabilities that those same technologies may create and be prepared to address, proactively and in an effective manner, those elements of risk mitigation and security that we should practice.

I told you I'd be brief. I didn't sing either. Thank you for your attention. I look forward to participating in this panel and hopefully having a good dialogue with the crowd as well.

MR. BORENE: Thank you, sir. (Applause.)

MR. MAGOFFIN: That's because I didn't sing, right?

MR. BORENE: Our next speaker is Mr. Kenneth Rapuano with MITRE Corporation.

KENNETH P. RAPUANO: I'd also like to thank LexisNexis and Andrew for the invitation to this event. I won't claim to be an expert on open source. I think as Dan said, we've been doing open source in perpetuity. You don't do intelligence without combining it with information that's available to everybody.

I think what makes it different today is really, again, this astonishing level of access to information on an immediate basis that we have today. I have a hard time managing Dan's charge to think 20 years from now because I have a hard time getting my arms around it today, in terms of what we have available.

I have four children, from 13 to 18, and they demonstrate to me every day how little I know about connectivity and the latest advances in information technology. It is the best of things and the worst of things, in a sense. And I'll again come at it from the perspective of a parent. We all know that the Internet provides new horizons for our kids in terms of the accessibility of data information. I also say it is the equivalent of a very large sewer pipe that's backing up to your house in terms of the potential of misuse.

So when we look at it from a blue-side adversary set, from a counterterrorism perspective, it's the same. We know for a fact that terrorists – al-Qaida, even Taliban, lesser organizations – are exploiting open-source information.

I won't get lost in the semantics of, you know, what's the line between open source versus all those other categories of gray information for which there are varying degrees of protection. I think the reality is that that band of gray is going to get larger and larger because what's immediately accessible to people is not necessarily what they're authorized to see. And when you get primary and tertiary levels of information that come into the possession of both adversaries and the blue team, you've got challenges on both sides.

Just to cite a reference, when you look at the '05 al-Qaida plot against the financial districts in the District of Columbia, New York City and New Jersey, a very sophisticated application of information that was available to them – obviously, from their on-site surveillance, but from exploiting data that exists on critical infrastructure, building plans, et cetera. That was '05. The availability of that type of information has only increased, notwithstanding safeguards that we are attempting, as a federal government working with state and locals and the private sector, to build.

When I deployed to Afghanistan as a Marine Corps officer as part of a joint special-operations task force, we did a lot of exploitation of electronic media that we pulled from individuals of interest. So the Taliban and al-Qaida elements who are described often in the media as running barefoot through the mountains with AK-47s – we pulled out of hard drives detailed transcripts of testimony to the Senate Select Committee on Intelligence, to the House Homeland Security Committee, GAO reports.

You can imagine the level of detail of information that we provide to potential adversaries. On the one hand, it's the nature of our open society. We want to maintain that. On the other side, we have got to maintain our comparative advantages.

And again, to Dan's point, we have some unique challenges in terms of how well we can exploit open-source and gray-source information. Two basic functional examples in terms of – from a domestic counterterrorism or homeland security perspective – threat analysis and then also threat identification, actor identification.

Threat analysis, broadly – what can we find out about different groups, about different thought patterns, about different potential targets? Then threat identification and characterization, individuals of interest and then pattern analysis. Pattern analysis is probably the highest-growth area for the exploitation of open source, I think, from both sides of the equation – the away game

and home – but particularly from the home-game perspective because of the increasing availability and amount of information.

On the other hand, there are lots of liabilities, in terms of the government's ability to do it and its willingness to do it, based on a whole host of privacy and other legitimate concerns. I think that we are only in the early stages of maturation in terms of getting our arms around that.

When you look at some just basic challenges associated with open source – I mean, I break it down in a way I think a lot of others do. The first is fusion of data. We are literally drowning in data, data that has potential nuggets of gold in terms of our ability to decipher and identify threat patterns and individuals of interest. We have got to do a better job of fusing it, filtering it, prioritizing it and disseminating it.

And then there's the big piece at the end, which is about the governance – responsible governance of how the information is collected, how it's disseminated and how it's used. How it's fused as well because there are lots of different colors of information: information collected by state law enforcement, information collected by the intelligence community, information collected by private corporations. A lot of it gets intermixed and trying to define its pedigree at different points in the food chain becomes extremely difficult to do.

Yet my concern – and I'm a tremendous advocate of fully exploiting all the information available from a homeland, national security perspective – but my concern is that if we don't responsibly address the governance issue, we will wind up dealing with a continued frustration in terms of our ability to exploit.

So there is a trail littered with carcasses of previous programs instituted by the federal government. Most of you have heard of TIA, the Total Information Awareness program that was instituted by DARPA in, I think, '01, or right after 9/11. This was about the righteous objective of collecting as much information as possible, fusing it in order to identify individuals of terrorist concern.

Yet they did not cover all the bases, both in terms of their communications policy, probably in terms of some of their personnel selections as well as their execution. It failed miserably.

There are others, the Matrix program, which was another – I think, early '00 program by a private company down in Florida. They did, again, threat analysis of open-source information. They worked with the U.S. Secret Service. They worked with DHS. They worked with the INS. I'm sorry, DHS didn't exist then. And they worked with the Florida state police. Ultimately, reportedly, they identified 120,000 names of interest. And apparently, the Florida state police actually made a lot of arrests based on the information. But that program also died.

CAPS 2 – that's the predecessor of Secure Flight – was a very sophisticated algorithm. And it was designed with a lot of privacy considerations in mind, in terms of porting over data on individuals to the private sector, the private sector running them through different levels of adjudication. Does the address of the residence the individual provides on their flight information line up with what's available out there on Ethernet? And a whole host of other alignment issues.

Critical value – when you look at 12/25, Abdulmuttalab, when you look at the threat that continues with regard to aviation, we need to be exploiting all the means of pattern analysis as we can. Yet it didn't make the vet. So we've had a real troubled record of performance in terms of our ability to achieve the balances.

And I won't pretend that I have the magic solution either. But Moore's Law is applying every day, in terms of the scale of information that's available and that we're collecting is totally outpacing our ability to analyze it, fuse it or effectively disseminate it. So unless we rely increasingly on more sophisticated levels of automation, we're going to lose the game.

Yet automation creates a lot of concerns, with regard to what's going to spit out of the end of the spigot and what are the implications for law-abiding Americans. Where's the line going to be drawn on how the data is applied? Who's going to be the arbiter of that?

So we do have a lot of different levels of authorization and regulation between what the intelligence-community players can do, what federal law enforcement can do. When you get into the state and local sphere, though, much more of a jumbled mix in terms of authorities, policies and how they apply the data. So again, we're in that very early phase.

And from a homeland security perspective, most of you are probably familiar with the proliferation of fusion centers. There're about 72 of them right now and they are run by states and localities, supported by the Department of Homeland Security. And they're designed to share information.

You're probably also familiar with the Information Sharing Environment initiative that President Bush initiated, I think, in 2004 or '05, or earlier. That was to really dramatically change the paradigm associated with how intelligence and other information associated with national security is handled and to move from a need-to-know to a need-to-share.

Personally, I abhor that phrase because I think it does a real injustice to the need to protect a lot of information that we develop. But the point that it's trying to make – and it's an important one – is we are going to have to share information with a wider enterprise of stakeholders who are critical players when it comes to the homeland security and domestic counterterrorism mission.

So we have a lot of different pieces in play. Information sharing is a big theme. It's a big priority. You hear people throwing it about all the time. Open-source information overlaps with that significantly. There're a lot of different initiatives to better utilize information. But again, I think we're still at a very immature stage and there are lots of liabilities and mines in that path that we're going to need to be careful in terms of how we navigate them.

Otherwise, we'll wind up getting put farther and farther behind in terms of our comparative ability, vis-à-vis our adversaries, to best utilize the information, to – really, it's about detection, classification, identification, understanding and preemption of the threat. Now, ironically, that was the mission statement for TIA. So we've come full circle. And again, it's not about the objectives. It's about the execution. So hopefully that'll be some fertilization for questions to follow. But that's the end of my piece.

MR. BORENE: Thank you very much, sir. (Applause.) I thought you said you weren't prepared? (Chuckles.) Our next speaker is Mr. Alex Joel, who is the civil liberties protection officer at ODNI.

ALEXANDER W. JOEL: Well, on that cheerful note and very optimistic note about the state of our affairs, let me start. So I am the civil liberties protection officer. I've been in this position since the stand-up of the ODNI. My job is to work with intelligence-community elements to make sure that their policies and procedures contain adequate protections for privacy and civil liberties.

And it's not my job to do that alone. Obviously, there are offices of general counsel, offices of inspector general, intelligence oversight offices, departmental-level privacy offices and civil liberties offices, the Department of Justice. We have the Foreign Intelligence Surveillance Court. We have congressional oversight. So we have a whole, what I call infrastructure for protecting privacy and civil liberties.

In terms of how our intelligence-community elements conduct their activities, we have a set of rules for how we go about doing that – founded, of course, in the Constitution and some of our core statutes as well. And then we have a set of rules that apply specifically to the intelligence community that are designed to make sure that we are able to carry out our intelligence mission but also respect the constitutional freedoms on which our country was founded.

So this is what I call the civil liberties protection infrastructure that is designed to be flexible and allow us to continue to protect our mission – conduct our mission. And I think protecting privacy and civil liberties, it's very important to think about that as a mission imperative because we can't conduct our intelligence mission, we can't pursue national security, if we don't have the trust of the American people.

We have to have that trust in order to have the authorities we need – if you just want to make it very practical – have the authorities we need to keep the country safe. So we have to demonstrate that we're doing a good job at that.

So some of the programs you talked about did, of course, suffer from some issues, encounter issues. I will say that, you know, for example, the Information Sharing Environment – just to touch on that, that is something that was established in the IRTPA, the same statute that created the Office of the Director of National Intelligence, just to clarify that.

And an example of – just an example of something that has happened with a dramatic difference over the last few years is the FISA Amendments Act, where we've modernized entirely how foreign-intelligence surveillance is done with a very dramatic change to that statute. We've also updated Executive Order 12333, so that's been another major change. So there have been things that have been moving forward.

Let me just talk about the infrastructure in terms of how it applies to open source. So I mean, we've heard about changes already in technology, the fact that adversaries are using open source, the fact that there's a flood of data. What I want to talk about here is how what I just described as the civil liberties protection infrastructure – it's not perfect, we always have to look at it; we have to make sure that it's working properly – how it responds to what I call these new pressure points.

What are those pressure points? It is new technology. It's new sources of data. It's the new threat environment, so all of the folks here who have just gone have touched on those themes. And it is new authorities. It's the new way we've organized ourselves as a community and as a government to try to deal with these issues.

So how does that apply with open source? I mean, what's going on in the open-source world? Open source, as Dan described at the very beginning, is essentially focused – as we've just defined it in the ICD, as publicly available information, information that's available to any member of the public. So right away, people can start asking themselves: Well, if it's public, how can it be private? I mean, how can we have a privacy concern with public information?

So two very quick answers to that. One is that in this new environment, it's hard to tell what's truly publicly available. And the other is that even with publicly available information, our intelligence agencies have certain rules they need to follow. Just because it's out there in the public domain doesn't mean that intelligence agencies can do whatever they want to with that data.

For example, people who blog on political Web sites and express political opinions – that's not something you want intelligence agencies to start collecting a file about. You know, what you have said in a political blog about whatever your political views are, that's not the business of an intelligence agency to be focusing on. So that's just one example.

Another example might be making sure that an agency has a particular mission to pursue something. We have divided up our agencies and given them particular missions to do certain things and we have given them training and authorities based on those missions. And so we want them focused on what their mission is to do. And we don't want intelligence agencies out there straying far and wide beyond their mission.

So I just wanted to give you a sense – we've been working on guidelines, guidance to provide to our open-source practitioners. Right now, this is all still in consideration, but essentially, it's in the form of – it's going to be in the form of a checklist.

You know, we're going to guide them through some questions, making sure they determine, is it really publicly available? Do they need special legal authorization to get at the data? Is this really in their lane as an open-source practitioner or is this in the lane of some other part of their organization or a different agency's organization? Is this really related to their mission? Those kinds of questions, to sort of guide them through how to deal with a rapidly changing environment. You know, are they making sure they're not focusing on someone solely because of protected First Amendment speech, that kind of a thing.

So let me just sort of take a step back here and think about the future and where we've been and where we're going in terms of open source. I think one model that it's easy to think about and conceptualize the issues on is if you think about the Foreign Broadcast Information Service and where this sort of started out, back in the World War II era and pre-World War II, when people were focusing on foreign-language news broadcasts.

They were listening to those foreign-language news broadcasts. These were specialists. They were trained to listen to those broadcasts, translate the news from those broadcasts, circulate the highlights for people who they thought would be interested in getting those particular news broadcasts.

So when you think about it, who was doing the broadcasting? They were mainstream news media of the day, government propaganda, those kinds of folks. What were the topics of those news broadcasts? You know, military, political, government, economic affairs – that kind of stuff. I mean, there were other topics, but that was generally it. Who was listening to that from the intelligence-community perspective? Trained, you know, dedicated, specialized folks who were monitoring those broadcasts.

Okay, let's switch to today. What are we doing now? Who's doing the broadcasting? Well, we've just heard and we've seen them. We all know about that. I mean, that's an obvious question: everybody, anybody. It's a lot of individualized broadcasters, right? And I'm going to use that term "broadcast" loosely. But there's a lot of user-generated content.

What's the topic of the broadcast? Well, of course, we've still got the mainstream media and people are still blogging and writing about issues of the day. But there's also a lot of personal journaling going on. Sometimes they're writing about, or blogging about or posting video about other people, other individuals. So it's a lot of individualized broadcasters, broadcasting on individualized topics.

And who are the consumers of those individualized topics by individualized broadcasters? Well, we still have open-source professions, as Dan was just describing. But we also have people in the intelligence community who are doing their day-to-day work, who now have, of course, access to the Internet, just as they do at home and just as we all do here. And they are going to access the Internet as they should as part of their work.

And so now we have a broader array of consumers. Now, if you fast forward – and we have technology that runs through this that allows for networking and interaction – a lot of interactivity among all of these folks in new and different ways and unpredictable ways.

And if you now fast forward this 10 years, what can we imagine is going to happen? Well, we saw some speculation. I think we're going to hear some more. As a civil liberties protection lawyer, officer and attorney, my thoughts on this are, I'm not going to try to sit here and ask the community to write one-size-fits-all, substantive rules today to deal with the technology that we see today. What we can do is provide a framework and guidance for dealing with these issues based on the principles.

I mean, there are a couple of ways that you can go about doing this. One is you could try to wipe the slate clean and start fresh. You could try to write technology-specific rules to attack specific technologies and say, this is how you're going to do it here; this is how you're going to do it there. The sources of inspiration that I think I'll just throw out there – there are two. One is the Constitution and one is the National Intelligence Strategy. So those are two sort of different orders of inspiration.

In terms of the Constitution, you look at – I want to get the words right here – not the Constitution, but Justice Brandeis in interpreting the Constitution. He wrote a famous dissent in the Olmstead case back in 1928, which dealt with that crazy new invention, the telephone. And in that case, they held that wiretapping the telephone did not require a warrant under the Fourth Amendment. It was not overturned until the 1960s.

But he said it did and he analogized a phone call to a sealed envelope. And when he did that, he said time works changes and brings into existence new conditions and purposes. Therefore a principle, to be vital, must be capable of wider application than the mischief which gave it birth.

One of his points was that we have to reason by analogy. You don't need to rewrite the rules as long as your principles are technology-neutral, they're protective and they address a fundamental aspect of human nature that is immutable – essential, that will not change, or is likely to change over time. Technology will change quickly. Human nature, not so much.

The other source of inspiration that I would like to point to is the National Intelligence Strategy. It's not, perhaps, on the same level as Justice Brandeis and the Constitution. But its vision statement – and you can see it at www.dni.gov – the vision statement provides, I think, a nice, concise way forward.

It says the IC must be integrated, a team making the whole greater than the sum of its parts. We must be agile, an enterprise that's adaptive, diverse, continually learning, mission-driven, embraces innovation and takes initiative. And we must exemplify America's values, operating under the rule of law, consistent with America's expectations for privacy and civil liberties, respectful of human rights and in a manner that retains the trust of the American people. So integrated, agile and exemplifying America's values.

I think integrated – we have to all get together and on open source figure out how we're going to tackle this is a community, so that we don't have a lot of different approaches across the agency, but an integrated approach. Agile, meaning let's not try to set in stone today exactly how we're going to do it, but let's remain agile and flexible as the technology changes over time. So let's stick to our tried-and-true principles and be technology-neutral about how they apply to a rapidly changing environment.

And of course, we always have to exemplify America's values in terms of protecting privacy and civil liberties. So let's stick to those principles, apply that framework to the way the technology changes over time and remember that we have to always have the trust of the American people if we're going to do our jobs. So thank you. (Applause.)

MR. BORENE: Thank you very much, sir. Our next speaker is Mr. Kevin O'Connell, who's an adjunct professor at Georgetown and CEO and president of Innovative Analytics and Training.

KEVIN M. O'CONNELL: Thank you Andrew, very much. Good afternoon, everyone. It is sometimes pleasant and easy to follow a panel like this. I think this one's going to be a little harder. What I'd like to do today is to offer a couple of thoughts about the future of open source in the 2020

time frame of my own and then try to summarize some of the thoughts we're heard today in preparation for your questions.

What does the open-source world of 2020 look like? Let me just offer a few big ideas that we can debate later on. First of all, there's not a single issue of intelligence or security interest – national or homeland security interest – that cannot be discovered – about which interesting information cannot be discovered in open sources of information. That's one.

The second – and I think we've heard the tensions here this morning – is that open source, which we've often thought about in purely a collection sense, really is much more about the merger of collection and analysis. And in essence, these two functions, whether we look at them today programmatically, politically, substantively, cannot exist without one another.

It will be absolutely much more analytic. We should talk more about the tensions that exist because the analytic points are the points at which there are certainly political concerns. And absolutely, there are substantive challenges.

And why is this important? One of the reasons that this will be important is that we in the intelligence and defense communities have talked about a concept we've called persistence: the notion of basically following a problem, a target, an issue, with almost constant coverage sufficient to actually explain what's going on, to get insight into what's going on.

The problem is that if you take the sometimes arbitrary line between open and closed sources of information away, we've got persistence. We don't need any other systems to worry about this. We've actually got it and that's been reflected, I think, on the panel in terms of the crush of data that we deal with every single day.

There's a real problem analytically in this world, though, which is that in a persistent world, anyone, a student, a politician, a decision-maker, an ideologue, can reach into that ocean of information and find any 10 pieces of data that, loosely coupled together, prove any point on Earth that they'd like to prove.

And that's going to put a real premium on analysis and frankly, very old-fashioned hallmarks of analysis, asking the right questions, critical thinking, effective writing. And I'll come back to that in a little bit. That's certainly another dimension of 2020 timeframe.

The third one is that, as I've written about, the seams between – there are emerging seams, I should say, between every one of the classic intelligence disciplines and sources that are open in the open world. I've written historically about commercial satellite imagery for which there's an entire new industry of people for which we can go out in the hallway and buy a satellite image on the backend of a credit card, okay?

Every one of the INTs has a seam at which it bumps up against a classic intelligence discipline. In terms of Dan's challenge to ask how we're going to manage this in the future, one of the things we're going to have to think about is how to not fight that seam as an intelligence function and actually leverage it to go – to move forward. That's another dimension.

Another one that's been spoken about at this table extensively is the notion that we're in an aerodynamic change with our adversaries, that they're going to learn a lot of information very, very rapidly and we're going to have to learn it as rapidly, if not more. Now, what's the problem with my description of the open-source world of 2020 is that it's really the open-source world of today.

Every one of these phenomena exist as we speak and one can only imagine that these tensions are going to get harder as move to the world of 2020, every single one of them. And so I hope we talk about these in the session. Let me – in some attempt to do a little bit of summary talk about a couple of questions that I've heard pop out at this table.

Dan started by talking about the notion of open source as a rigorous analytic discipline. I couldn't agree with that more. But to have that discipline, we're going to have to continue to build in our educational system the kinds of skills to be analytic and rigorous about our thinking.

I gave a briefing to the Defense Science Board about six weeks ago on which we talked about critical thinking and effective writing and asking the right questions and things like that. It sounds very old fashioned and I guess I'm wearing the professor's hat at the table today so I'm allowed to say this, but absolutely essential if we're going to do this right. Okay, that's one dimension of it.

Someone asked the question, does the advantage necessarily erode? One of the myths about – one of the myths about open source is that in the open source world, secrets don't matter. That's nonsense, okay? They matter, but they play a very different role relative to what is openly available out there.

And we have to make that transition in how we manage ourselves as an intelligence community and frankly, as a society. Secrets will still be important but they'll be different and they'll be gotten in a different way. This question of dealing with how the adversary takes advantage of the data that's out there.

It's a very thorny question and I often take interest in the kinds of solutions that people propose to do that. One of the tensions that exist in this world is the tension between the desire to control information – and this is, of course, the last building in the world that we should be talking about that, but controlling information and actually making use of it on the other side.

That is a real tension and the temptation to want to control is very, very strong. I think we have to think about it in a slightly different way, which is to assume that the information is already out there for many of the things we worry about. If it's not out there, then we can assume some interest in control.

But a lot of data that people need to cause us harm is already out there. And remember another uncomfortable fact that the threshold for information that other people need to do us harm is often a lot lower than the information that we need. If the U.S. Air Force wanted to come in here and get all of us, they'd make sure that they didn't burn the plants down that are sitting behind us on this panel, okay? With that kind of precision.

A terrorist group has much less interest in worrying about things like that. And in fact, they would rather take out the whole neighborhood if they could because of the political effects. So the notion of information control and its value in releasing it or keeping it back is something we have to think about very, very carefully.

Obviously, at the table today, we've talked about a number of unique challenges. One set of them is internal to the intelligence enterprise, how are we going to deal with these – what I've called the seams? The governance issue that Ken raised is very, very important. We all have seen at this table – we all have seen initiatives that were very good and innovative and for want of some issue related to governance, they feel by the wayside. That's unfortunate.

We can't let these innovative concepts be destroyed before they're actually born out to show the value of the open sources. And then to Alex's commentary, we're also going to have to adapt to this as a nation and think about how these rule sets – and I don't mean the Constitution here, of course, how are these rule sets going to change in a world where there really are separate rules for the government?

And you've all heard before this notion that in the commercial world, we're willing to give away every single piece of information about us and let other people use it to their effects and perhaps our own benefit. We take a very different view of it when the government starts to look at that data.

Somehow, that thinking has got to adjust. It doesn't have to be black or white, but it's going to have to adjust in a direction of the future as it has been envisioned by everybody on this panel. And on that note, I'll stop and I think we're ready for questions. Thank you.

MR. BORENE: Thank you very much, sir. (Applause.) Thank you very much, gentlemen. I think you really did an excellent job laying out the situation and the mission before those of us with an interest in this as a field and the five-paragraph order format, that the execution, administration and logistics is really up to those of us that can collaborate and have conversations to come up with innovative solutions, really across the spectrum of – it was mentioned, government, private sector and academia.

So that said, I'd like to open it up to questions. And before we open it completely to everyone's questions, if there are credentialed media in the room and there are press questions, it is the National Press Club, as referenced before. In honor of the First Amendment, I think we would ask if there are any press questions first. Yeah, yes, sir. And if you could wait until I bring the microphone to you, I would appreciate it. In fact, I'll repeat your question on the microphone.

QUESTION: (Inaudible, off mike.) It sounds like a lot of what you're talking about is overwhelmingly like a – (inaudible) – when you're – when you're looking at decisions, how much information – (inaudible). It sounds like, you know, everyone – almost everyone's trying to say there's just too much room for the analysis, so you know, I'm writing a story. I should have a – (inaudible) – what I'm going after, so why not make that decision – (inaudible)?

MR. BORENE: That was Ben Bain with Federal Computer Week. Sorry, apologies, I'm sure the transcript will get it. I think what I will do is pass the microphone to the next question. (Laughter.)

QUESTION: Why not make decisions ahead of time – (inaudible, off mike)?

MR. BORENE: So the question is the balance between information and technology.

MR. RAPUANO: I'll just say I think it gets back to what's the purpose – what outcome are you looking to achieve? And I think folks recognize there are a lot of different sub-missions within the open source intelligence realm. So if you're trying to scan the environment of available information, then you've got to do the full net.

If you're looking for particular elements of information, then if you have the ability, you can be more selective in terms of targeting the nodes where you're most likely to get what you're looking for. But then you need that – you need that understanding of where to look for it. If you don't have it, then you're stuck to your wide search.

MR. BUTLER: Yeah, I think I'd add – if I could, I'd like to add to Ken's answer, Ben. I think we do what you just described. And I think Alex Joel made reference to this. The various parts of the intelligence community have various missions and authorities. By virtue of those authorities, or limits to their authorities actually segment what they do go after. And they do segment very carefully because they have to be efficient at what they actually search for before they can begin to grapple with that torrent of information that Mark Gabriele was talking about earlier.

MR. GABRIELE: Just to further address that. Yes, there are torrents of information, but the information continues to flow, okay? So sometimes, you can think of the Internet as sort of a giant repository and you can go back out and get the thing that you were looking for because it was there last year and the year before and the year before that.

Sometimes, it's not there forever. Lots of information on the Internet is ephemeral. So I see something which is of intelligence interest, is of, you know, potential probative value in the future, darn right, I want to get it and I want to hold on to it. And when I get it and hold on to it, then I want to make sure that it is indexed, catalogued and that I've processed it and teed it up for processing against future bits of information that are going to come swimming my way, okay?

So it's not – I don't want to capture the entire Internet and have it always with me in my back pocket. It's not practical and it's not productive, but I do want to be selective, certainly. But I need to hold on to stuff if it looks interesting because I don't know what's going to be there tomorrow.

MR. MAGOFFIN: I'd throw out one thing as well. I mean, it's – there's the emphasis on the Internet for obvious reasons, but you know, an open source is obviously much more than that. There's many sources which currently don't reside on the Internet – newspapers, radio, television and those are equally important as well.

I think that the challenge is, is when you obtain the information from those disparate sources is then how do you aggregate it? And then how do you place it in a format which is easily analyzed? So there's always a tendency to rely upon technology or use technology as a silver bullet. And quite

frankly, there's always a human in the loop. There always has to be those temporal processes going on. But again, just a disclaimer that there's still a lot of open-source which is not Web-based, so.

MR. BORENE: Sorry, Mr. O'Connell?

MR. O'CONNELL: Just one quickie in response to your question. The – you know, I think you're one of the examples of the issue at this nexus of open source and analysis as we've talked about it. There are a lot of issues which are emerging which we really don't understand analytically.

And oftentimes, your ability to understand that analytically can come from collecting more data. But it oftentimes comes from a human being who has followed an issue very specifically. I think in your packets, there's an op-ed I wrote about a year ago that talks about this relationship between open source and analysis.

There are a lot of phenomena in the world that people know that they've reached the outer edge of analytically and the only people that are going to give you a clue as to what to look for in that crush of data are experts that follow it on a daily basis. They're typically not in intelligence services either, those folks.

MR. BORENE: Yes, sir?

QUESTION: Thank you. I contribute to the Counterterrorism Blog, but my question really goes back to – during my many years in the State Department Counterterrorism Office, I and a lot of our officers paid a lot of attention to press reporting because quite often, we thought stories from good correspondents – I'm biased because I used to be a foreign correspondent – had information that was not contained in the agency or embassy reporting.

And I was wondering – are you seeing any impact from the cutbacks in the media – the number of foreign correspondents overseas, especially the American media? And second of all, in looking at open sources and you know, some of it comes from monitoring, I assume, still, if they mention things in government-controlled press in many countries, via the old, what used to be called the Foreign Broadcast Information Service that's subject, perhaps, to disinformation or distortions or CI ops. How much is that a factor when you're trying to filter out what's going on?

MR. MAGOFFIN: I just want to try the first part of your question. I'll leave it to the larger heads on the table to take the other one. (Laughter.) In terms of U.S. foreign correspondents overseas, I think to some degree – and not to contradict what I just said about sources not all being on the Internet, but some of the proximal access requirements which we once had, where we had to have folks overseas to collect data.

In some instances, through partnerships as well as through technology – some of the emphasis or the need for those – for that proximal access had gone away. And that's even in the case of television and radio. So your question was, has there been a negative impact? I suppose in some aspect of open source and in the larger media operations, I'm sure there has been. But insofar as trying to examine foreign media to get a sense of what's going on in regions in other countries, I'd say no.

Where I think the United States, in particular, sometimes struggles is in researching or consuming that media in vernacular. And I see one of my compadres in the audience, who works with the language authority at the Defense Intelligence Agency who works machine translation and the like to overcome some of those obstacles which we face.

You know, being unilingual and barely that with English, I mean, I'm no one to say this, but we obviously have to do better in that arena and through technologies and perhaps, you know, as part of this particular form, in 10 years and that's certainly the forecast is that a lot of those tools will be better.

So a long-winded response to your one question, but you know, we probably could use more folks overseas. But in terms of the collection, I'm not so sure is the negative impact is as significant as, perhaps it might have been before the Internet and other technologies.

MR. BORENE: Mr. O'Connell?

MR. O'CONNELL: I think the gentleman's question actually puts a nice new optic on open sources and one of the interesting things about open source is that when you look at it, you can see it through so many lenses. You're, again, on the human dimension of this, at least in my view. I do think, in answer to your first question, there has been somewhat of a decline.

But it also points to the fact that while we're talking a lot about data at this table, what open sources often provide is the kind of context – the rich picture – that analysts do not have. If you're sitting inside one of the agencies and you've got barely a master's degree and you know, a passionate interest in energy, but you've never lived in the Northwest Frontier, these are very helpful sources to help you understand how life is lived and people have expectations and day-to-day activities take place to do that.

So it's not, here in this context, such a data question as much as, how do I paint the picture? The good news is that there's nothing sensitive at all about that kind of information. But it is absolutely essential to having analysts do the kinds of work that they do. I've never known a good analyst in my career that didn't understand the lines of the currency, debate and discussion on a given issue, ever. And a lot of that can be gained from outside sources.

MR. BORENE: Anyone else want to comment on that?

MR. BUTLER: Well, I would just say that Mike, in answer to your first question, there's no question that there's been a significant cutback in traditional media, overseas correspondents and it is has an impact on the quality of traditional media. You just have to hold your Washington Post every morning now and you know it's a lot thinner and a lot less weighty.

I think also the quality of the reporting has suffered, not just print media, but broadcast media. And that's a personal opinion. I'm not giving you the ODNI opinion, necessarily, the vetted ODNI opinion, but the very first two pieces of open source I look at everyday are Channel 4 to see what the traffic's going to be like in D.C. and I read the Washington Post.

And I've been discouraged at how traditional print media has deteriorated in terms of breadth, depth, content, quality. And that's unfortunate because that was an extraordinarily good source of information, I think, for our policymakers, unmitigated, not mitigated, unmediated by the intelligence community. But also, it's an important source for the intelligence community analysts.

MR. BORENE: Yes, sir?

QUESTION: Yes, thank you. I'd like to ask about the two-week – yeah, okay, I'm an adjunct professor and I have my own consulting firm. And I've been teaching a course on the intelligence community to undergraduates for the last dozen years. It's amazing how much information has become available via open source since that period of time.

Point – one of the things about the intelligence business is that you really don't want the other guy to know what you're interested in. And I'm concerned about what you might call the problem of the cookie counter. You leave a trail. When you start doing research, you leave a trail. And the smart guys are going to figure out where that trail is leading. Is there a way to deal with this? This is along the edge of cyberwarfare, I recognize, but I think this is one of those concerns that we can't ignore.

MR. BORENE: Anyone want to –

MR. O'CONNELL: So the question was, is there a way to deal with it and the answer is yes. And I think that go into much greater detail than "yes" would probably get me in some sort of trouble with some people in this room. (Laughter.) So suffice to say, the answer is yes, there is a way to deal with that.

MR. BORENE: Question? Yeah, yes, ma'am, sorry.

QUESTION: Thank you. Hi, I'm a private citizen. I work at Walter Reed but I'm not speaking for the Walter Reed Medical Center. I have a question I think either Dr. Joel or Mr. Magoffin or Mr. Rapuano might be able to answer this. I'm not sure, but you have to pardon my Boston accent. If you don't understand anything, just let me know.

(Cross talk, laughter.)

QUESTION: See? You do speak a foreign language. How do we find a balance between the constitutional protections for privacy and using open source? Open source is open source, it's international. The Internet is international. Bad guys don't play by the same rules. They don't have our Constitution. And if it's in the open domain, what is the problem with tracking a blog that is a threat?

Either it's a domestic blog or a Taliban blog or whatever kind of bad guy blog there is, tracking that and exploiting it? I don't – I guess because I'm a very junior analyst and have done some analytical work as well, that I don't see a problem with exploiting everything we can relative to the Internet simply because it is in the open domain. I mean, it's just all over the world. And what are some of

the issues and how do we not hogtie ourselves to the point where we can't use or share the information interagency?

MR. JOEL: Okay, so I don't want to get too much into the details in terms of the guidance that we're working on, but in general, there's a lot that analysts can do in the open source domain. I mean the information, once you're satisfied that it is publicly available, there is a great deal that you can do with publicly available information, just like any other member of the public can –

QUESTION: (Inaudible, off mike) – bad guys?

MR. JOEL: So you're asking about domestic – so let me just – so I'm giving the general – first, let me – so in general, if it's publicly available, you can. Now, the First Amendment does exist and that distinguishes us from some other societies. We have strong First Amendment protections.

And what the First Amendment, in general, covers here is, in the blog context, is speech. So just because someone is saying something on a blog – just like if someone were saying something in a street corner, the U.S. government can't just come in and start monitoring it. So if someone was protesting policies of the administration, be it this administration or the prior administration or Congress and they're protesting it even in extreme terms, that, by itself, is not a reason for the government to start monitoring, taking a file, starting, you know, taking your name down and putting that in a file or anything like that.

It has to bleed over into something that we believe is violence, you know, goes into the incitement of violence. So there's – there is some Supreme Court cases on this and it gets into, you know, we're working on providing more detailed guidance on how to, you know, where does that line cross?

So there's a First Amendment consideration for the U.S. government in general. In terms of the intelligence community, there are different agencies with different authorities. Some can look at stuff inside the United States like the FBI. Other agencies are supposed to be focused on foreign threats.

And of course, the First Amendment applies to stuff that happens inside the United States and to American citizens and United States persons. It doesn't protect people with no American connections who are located overseas. So that's, in general terms, how we would provide that guidance.

And we're trying to write it in a way that's very clear and that can be used by, you know, intelligence community elements, but also is flexible and allows for people to know when to consult with their attorneys for more detailed guidance. So it's not easy to write. (Laughter.)

MR. BORENE: Thank you, Mr. Joel. Any of the panelists want to – Mr. Rapuano?

MR. RAPUANO: I would just add that it depends on – it depends on what you intend to do with the information. If you intend to use it as actionable intelligence, then a number of the points that Alex just made apply. Taking into account that there is a world of gray. So if you're expressing

your constitutionally protected right of speech, you know, when does it go from being vitriolic to be potentially fomenting violence?

If you're planning a protest at the Pentagon the next day, what's the responsibility of the Pentagon protective authorities or the Arlington police to monitor what's going on in that blog? Talking about logistics, talking about people coming, that's all great. They're going to bring flags. Oh, now, they're going to bring tear gas – so – or mace, so all of those lines are drawn and there are case precedents in the rest.

But we are in a brand new world in the sense of – I think there are cultural elements as well. If you talk to young people today, their expectations of privacy are quite different than older generations. You know, I keep telling my kids anything you put on the Internet, you ought to be prepared to go anywhere and they professed to not be all that concerned about it.

Now, they haven't been bitten bad yet – (laughter) – and that life experience will do that – but I do think that there is a shift in cultural perceptions of you know, what privacy – look at these Twitter – GeoTwitter sites. People are constantly – let's say you're on Twitter Geo and you've got 1,000 friends following where you go, but you've given them individual permission, well, can the federal government follow you if they have an interest in you based on your Twitter feed? So I mean – these are things that are happening in real time and there are a lot of – there's a lot of work going into it at both the federal and the state levels. But it gets to the complexity.

And the last piece I'd mention is this risk perception issue. Prior to 9/11, you would never have had the Patriot Act legislated because the public perception of risk was not sufficient for them to be supportive of the type of invasive aspects that some would claim the Patriot Act authorized.

So this whole perception of risk in how authorities communicate risk is a real fundamental component of how we go forward. You know, what's the benefit? There's no free lunch here in terms of the national security aspects. The more we want and need to find out about what unknown actors are doing, the more potential risk to privacy.

You can't have it both ways. You can put a lot of protections in and you can balance it and you can govern it judiciously, but it's never going to be totally free. So that's, I think, what we're in the midst of and there's a lot of good work going into the development of guidelines and the rest. But we're just trying to keep up with the technology in terms of, you know, the new doors that open and the new complexities that arise in terms of, well, what about this particular case now that this capability is out there?

MR. BORENE: Mr. Butler?

MR. BUTLER: Yeah, Ann, good question. I think what I fear more is that individual analysts who do their own open-source exploitation will hogtie themselves because if they're professional, they're conscientious, odds are pretty good in our intelligence community that they will be afraid to go where they can go, where they're authorized to go, where they should go, where we expect them to go in the performance of their duties.

It's why the guidelines that Mr. Joel is working on with his CLPO colleagues around the government are so important because we want to enable every intelligence professional to be able to know and be confident that know that they can go up to the line without going over the line. And that's why making sure that every intelligence professional is an open-source exploitation professional is – and that as a core competency is a high priority in my view.

MR. BORENE: Question in the back here, waiting a while.

QUESTION: Hi, I'm with the Library of Congress. And I have a question, Doug, there was a comment you made and then this gentleman to let you know we also have a way of dealing with the non-traceable IP address. (Laughter.) I'm with a group that actually does open-source research.

And my question here – and it gets back to a previous question is about we are overwhelmed with requests for multilingual, multicultural – people who understand this. And what I see right now – I speak daily with people in the intelligence community, both civilian and DOD. And what I see now is a real dearth of people who are savvy with the cultures.

And someone who – we got one project where we actually had to sit down and decide – we cannot have a person do this project who grew up in this country because it had to do with a tribal issue and we were too concerned about their biases. And these types of things are so critical and so important.

And it seems with the – that there's a huge shortage and then also, a lot of the material is in the native country and unable to get access to it. So I'm just curious how – I mean I know how we deal with it. We have our overseas offices we talk to, but how is the intelligence community addressing that because that's a pain point I see on a daily basis?

MR. BUTLER: Ann, good question, thanks. Actually, I just spent an entire day on Tuesday at Georgetown University listening to 12 different scholars at Georgetown, all of whom were naturalized American citizens who were providing presentations to me and a number of other folks in the audience.

In fact, Library of Congress was represented there – the federal research division, which I presume that's where you're from. And it was remarkable. The quality of the research, all open source, and the quality of the analysis that was done by these scholars – I was almost tempted to say young scholars, but some were in their 50s, was impressive.

And they went through an eight-month boot camp – I'd call it – at Georgetown, funded by the U.S. government to specifically address that concern of yours, to try to get into the national security arena, working our mission on behalf of the United States, people with native fluency in a language and cultural understanding that is also native – that you can get no other way than by growing up in a foreign country or foreign region.

And they had very interesting perspectives that the typical American-born analyst in the community would not have or would not appreciate. So we are doing things to try and invest in that type of capability, bring that kind of talent into the government. We, actually, this year, asked that the

National Security Education Program, which funds that program, double the size of the program from 30 students to 60.

And in fact, the Washington Post recently carried an ad for this particular program. It's called the English for Heritage Language Speakers Program. And I think it has the potential, over time, to help with that program that you've identified.

MR. BORENE: Mr. Magoffin?

MR. MAGOFFIN: How are you doing? I remember when you came over to chat about six months ago. We – now, this is the future, but I will caveat to say how we're doing it now and I think, again, on the Iraq experience and Afghanistan experience, a lot of you are well familiar with how we've done it.

We've done it through contractors. We've done it through vendors. We've done it through independent contractors. We've also – as I mentioned previously – we've relied, to some extent, on machine translation when it's possible, not necessarily to translate documents or websites, necessarily, but to provide a gist, an idea of what the content is all about it.

Obviously, when you're taking the human element in, you've got to have another person there standing in front of them, talking. But there's also an increased emphasis within the intelligence community to grow language capabilities on our workforce. And those efforts are expansive, not just to grow it, but to maintain those capabilities.

There's also increase, and I think, enlightened activities to hire those types of capabilities for government service as well. I think what complicates all of those activities. And it's analogous to the information problem that we have – it's everywhere, it's ubiquitous, it's huge. Well, so is the world in which we're looking at and we're concerned with.

And on any given day, a country can come out of nowhere and be a top priority for national security. So how do you take these finite resources and allocate languages if you could? You'll be a Swahili speaker. You'll be a French speaker. I know he speaks French. And I don't know if you speak Swahili. Okay. (Laughter.) But how do you break it up?

You know, how do you account for all of that? And it's just like we do most business, there's some risk entailed that you assume. But that is challenging to say the least. And again, it's part of our culture in the United States anyway, that there's just – there is a dearth of folks who speak more than language. So –

MR. BORENE: Mr. Butler?

MR. BUTLER: Yeah, let me add something else too, Ann. Doug reminded me of it. And I was remiss, not bringing this up – one reason we in the intelligence community feel it's so important to partner with academia is a vast amount of the expertise we require that we need or that we might need, we can't keep on the shelf, but we might need it just in time tomorrow.

As Doug pointed out, we can find that in academia. I mention Dr. Dick Ward earlier and Dan Mabrey, who is one of his protégés at Sam Houston State University. They did exactly this – Sam Houston State University – they built a capability to employ young, talented students, not from the United States in most cases who had native language fluency and they evaluated open-source information against various different issues and research topics that they were interested in.

And it was – I was impressed by it when I saw it and I think that is one of the things that we're going to have to figure out as a community as we govern our capabilities across the intelligence community and across the government. And we look for efficient ways to garner that kind of expertise and exploit open sources with that kind of talent, we're going to have to figure out how to partner more effectively with academia and with academics.

MR. BORENE: Go and make sure we get some questions from this side of the room as well.

QUESTION: Thanks, Andrew. I'm formerly with TSA and DHS, transitioning into the private sector. We've been dealing with these questions, of course, at the domestic level. As usual, there's a lot of talk here at the federal level and OCONUS. But even before you get to what people classically consider intelligence, the 56 states and territories and the 18,000 PDs have all got different definitions of what's public and what's not.

I was surprised in The Washington Post the other day to see that it's illegal in Maryland to tape a state trooper doing his job that was – came so – that indicates there may be a trend the other way toward making things more closed despite the ability to do it with the new gadgets rather than being more open, which is what we need if we're going to have any sort of domestic situational awareness.

Who's job is it to try to make a coherent national policy in these state and local jurisdictions that meets our needs in this post-9/11 world?

MR. BORENE: Mr. Butler? (Laughter.)

MR. BUTLER: I'll let Ken answer this one for you in just a second. Actually, I think it may be impossible to govern the ungovernable. And we talk about governance and I just blithely mentioned it myself a minute ago, but some things will simply be ungovernable and we're going to have to use those immutable principles that I think Alex Joel talked about earlier to figure out how best to take advantage of that kind of information, how best to accept that the federal government can't control everything and maybe we shouldn't.

Maybe there are – maybe it's a good thing that state, local governments have different authorities than we have. And certainly, they have different authorities that apply in a much more local sense to their problems than perhaps the federal government would need to care about. So I – I think it's probably a fool's errand to try to govern everything regarding state and local jurisdictions and put in place policies that we could even hope that they might follow. So I wouldn't be optimistic that we can do that.

MR. BORENE: Mr. Rapuano?

MR. RAPUANO: I would say that you put your finger on – and based on your experience in TSA and DHS, you're well familiar with the dynamic. One of the toughest aspects of the homeland security enterprise – and that's the division and delineation of roles, responsibilities and authorities. I share Dan's skepticism about how far this can go in terms of these are really constitutionally delegated authorities to the states.

But if you look at the growth of the fusion center functions and information sharing writ large, in the federal, state, local enterprise from a national homeland security perspective, there's going to have to be some better commonality of understanding as to what's transferable because otherwise, the system is going to really be degraded from all the chafe that occurs when data is traded.

And it's an issue right now in terms of there's a lot of information, for example, that the state of Maryland won't share with other states. It needs to be – there needs to be a special permission provided. So another state can say, geez, I think you may know something of interest to me in terms of an actor or a threat, but I need to specifically ask for it versus be able to pull it or have it pushed to me. So that's another one of the tough problems that –

MR. BORENE: And that's actually going to have to be our last question, so I wonder if any other panelists have any parting thoughts before we wrap up the afternoon. Nothing? Okay, I've got – or do you want to keep going until 3 (o'clock)? I guess we can –

MR. BORENE: We can take one more question – (laughter) – as long as – I think there's plenty of room for conversation to keep this going until 3:00 a.m., but maybe we'll take another – sure, absolutely, here you go.

QUESTION: Thank you. I am an OSINT analyst. On top of that, I'm fluent in five languages, since you guys were talking about languages. And part of the panelists were talking about the other side, looking at our open SINT, open source intelligence. I think the danger that we are leaving is the footprints.

The gentleman asked a question about the IPs. And the former DNI, Michael McConnell, he wrote the Vision of 2015. He insists that OSINT must be done outside the dot-gov, dot-mil environment. However, in all my years of doing OSINT, I was only able to convince DIA to allow me to do that between 2006 and 2008.

I was the leader of the Project Strider. It was awesome and I was doing OSINT in the middle of nowhere in the Rappahannock River. When I came out of the woods and I went to teach OSINT at ONI, I was shocked because they believed that the IP is secure, is not. So you cannot think that the anonymous IP is secure, now, the other side already has it.

So how are we going to deal with that? How can we push the other agencies to really understand that OSINT has to be done outside the dot-gov, dot-mil? And how can we teach en masse, the analysts that I was teaching. And they thought, oh yeah, I can do – I have my IP anonymous, so I'm going to check my personal e-mail, leaving a passport – or password – and they go on and check the other side? So –

MR. BORENE: Okay, Dr. Gabriele.

MR. GABRIELE: For the last problem, that, we usually resort to, you know, electric cattle prods, things like that are good inducements to analysts to keep them from doing dumb things. It's training, okay. So there is a lot of room for improvement in the way the intelligence community does many things.

And open source collection and exploitation is certainly on that list. And in all fairness, Mr. Butler has done a great job in dragging the intelligence community along, in some cases, in improving their open-source collection capabilities. That said, when you start talking about, gee, we need to make these minor improvements in your information infrastructure, oh, well, that means the CIO people get involved.

And that means – you know, there are a number of things that start to happen when you start talking about a computer – and it – oh, it's a computer that's going to be at an intelligence facility and oh my, the number of regulations that suddenly come out of the woodwork to thwart any useful effort can be sort of overwhelming.

So there has been progress made. There, I think, will continue to be progress made in that direction. I'm glad you raised the question because it is an excellent point and it needs to be – it needs to be recognized that – that there needs to be attention paid to open-source tradecraft straight across the board.

It's not just, put somebody in front of a web browser and tell them to go. It doesn't work like that. It is an intelligence analytic discipline and there has been a lot of strides made toward improving training for open-source analysts. A lot of that's been the effort – been because of the efforts of the DNI and the ADDNI for open source.

There needs to continue to be those efforts and they need to continue forward and the agencies need to pick up the ball and go with it themselves.

MR. BORENE: Anyone else on the panel? I just want to make sure that if there is credentialed media or members of the press club present, that we get those questions answered. Is there – are any? Nope. Yes, sir.

QUESTION: Gentlemen, good afternoon. I'm from the National Air and Space Intelligence Center. Mr. Butler, sir, I found it interesting that you discussed the WMD Commission report and seem to suggest that the need for open source intelligence analysts should go – eventually go away, that it should be subsumed under the greater all-source analyst responsibilities.

And given the discussion that the panelists had on the need for a discipline with a well-defined tradecraft so that we don't have people stepping all over each other and inadvertently destroying perfectly good sources of data, do you personally think that that is a good idea, that we eventually fall under all-source analysis?

MR. BUTLER: Well, first of all, I do think it's a good idea to aspire to what the WMD Commission asked us to aspire to, which is to raise the boats of every analyst in the harbor, get the core competency and capabilities of our analytic core across the IC higher when it comes to open-source exploitation tradecraft.

You did make note of the comments and concerns that – with the way things might progress over the next 10 years with the sophistication of technology, the techniques, the tools that we encounter – the tradecraft may evolve very, very rapidly. It should evolve very, very rapidly.

It's probably unrealistic to expect that every single analyst in the community will be trained to the same level of expertise. And that's one reason why we're working on a certification program right now within the intelligence community because we want to be able to certify a subset of the intelligence community as true open-source intelligence professionals.

And we've assembled the entire community. All agencies have been represented in this effort. And we have, I think, devised a pretty good framework, a core competency, a certification regime that will allow us to recognize that they will be the masters of the open-source universe forever, probably.

I think we will always have folks within the intelligence community that will exceed all others when it comes to their expertise and their focus and their sophistication in terms of tradecraft. They will be the people that will be actually doing most of the innovation, pushing the envelope and bringing the rest of the community with them. But I think that's ultimate goal, is to bring the entire community with them as they progress over time. That's how I would reconcile the two.

MR. BORENE: Yes, sir.

QUESTION: I'm president of the OSS Society in McLean and I'd be happy to stay here till 3 (o'clock) hearing you all speak. (Laughter.) It's fascinating.

But I'm listening to your comments, I was reminded of a couple of my favorite comments from OSS founder, Gen. Donovan, who tackled many of these same issues in World War II, when the U.S. didn't have a centralized intelligence service, which is one of the reasons why its original headquarters was the Library of Congress and why they went out and recruited lock, stock and barrel, literally our nation's best and brightest academics, historians, writers, artists and you name it.

In World War II, Hitler – and Hitler said of the U.S. that you know, racial diversity was a great weakness. And of course, Gen. Donovan countered by saying, in fact, it was our greatest strength because no other country in the world had so many citizens with knowledge of other countries. And I wonder today if we're not really tapping that resources.

And secondly, in one of his other comments – he once said of its research and analysis unit which went on to form the basis of State Department's INR that the major part of the success of OSS was the result of good, old-fashioned intellectual sweat. So I just ask any of you to comment on that in relation to the challenges that we face today.

MR. GABRIELE: It is not lost, I think, on any of us that you've asked that question of a panel full of middle-aged white guys. (Laughter.) Who most of us are looking at each other like yeah, I can translate into Bostonian – (laughter) – you know, okay. So having said that, I think that there is a surprisingly large amount of diversity within the intelligence community and I don't think there's any hesitation to take advantage of it. And I would – I would refer you to Mr. Butler for a discourse on the intelligence university program – what's it called? Going blank on this. The university outreach program.

MR. BUTLER: Oh, CAE.

MR. GABRIELE: CAE – thank you – Centers of Academic Excellence, which is, you know, intended, exactly along those lines. And it's somewhat more diverse than the panel that you see before you.

MR. MAGOFFIN: I think that – yeah, I think those two statements that he made years ago are still accurate and I think, you know, some of the other questions have been posed, kind of touched on various key points, which is, you know, diversity within the workforce and diversity in the sense, his cultural, his language, his experience – life experience, academic experience and all the like.

So you know, I can speak to, at least in the last 10 years, I can't speak – well, I probably could – but then you start giving ages away, I suppose, but in the last 10 years, I mean, there's increased emphasis, again, on bringing people in with the requisite skills, you know. And the analogy would be back when I was looking at information operations, was, you know, we had analysts who were not technical by training.

They were regional experts. They had languages and so forth. But they could not look at, necessarily, at electrical grids and communications networks and really drive down into the heart of those and understand them. And I made the statement – it's easier for me to train an engineer to be an analyst than analyst to be an engineer.

So it's always this – you know, it's always this formula, this ever-changing formula of trying to get the right mix of folks to, again, address a myriad of topics. And you know, to counter, as an Irishman myself, you all know that the Germans said about the Americans is that, you know, they're very difficult to fight because they don't read their own doctrine, right?

In this case, I hope that's not the case. I hope that we can document how to do this business and more importantly – and bring those people aboard that can – and perform these processes and very complicated and specialized processes, which unfortunately, there is no shortage of people that believe that open source is really, you know, going home and bringing up the Lowes' site and doing some cost analysis on weed-whackers, you know? Very difficult to try to dissuade those people that it is a complicated business, so –

MR. BORENE: Mr. Butler?

MR. BUTLER: Yeah, thanks. Thanks for bringing that up. Hopefully, through the tone of my remarks, it's become clear that I believe diversity is one of the things that we have to pursue

aggressively. When I talk about comparative advantage relative to an adversary, when I hear that mythical figure that there are more Chinese that speak English than there are Americans who speak Chinese, it concerns me.

I think that is one of the strengths of open-source intelligence. You heard Kevin O'Connell talk about how there's virtually nothing that we can't go out into the open-source universe to learn a lot about if we strive to do that. In fact, if we were to hogtie ourselves and say all you can use is open source, now find us the very best answer that you can provide to policymakers, I would venture to guess that we would probably provide pretty good advice to our policymakers, even subject to that constraint.

That, again, is one of the advantages of open source. We can reach into very diverse communities. We can reach into academia. We can work with foreign partners who do understand issues, perhaps, differently, better than we do and take advantage of that – that knowledge.

And we don't have to worry about clearances and classifications and barbed wire and blue badges and green badges, et cetera. So your point's well taken. And it's something that we're trying to take advantage of today with open-source intelligence.

MR. MAGOFFIN: Not unilaterally, with partners as well.

MR. BORENE: Mr. O'Connell?

MR. O'CONNELL: Just one other addendum on your – on the second part of your question, which is there's a whole parallel set of initiatives underway to help improve the analytic component of the story in the intelligence community. Intellectual sweat is something that most analysts unfortunately don't have the luxury of a lot of time to do.

What the quest is, for now, within the community initiatives that I understand is to really buy more time for those analysts to really put brain power on problem sets. And the extent to which we sacrifice that, we do at our own peril. You know, since you are obviously interested in the history, I'd point back to a fact of Dulles' arrival in Bern, Switzerland.

What Dulles did was to go around and talk to a lot of people, collection, but then he absolutely did analysis on the data that was there. You cannot have one without the other. And as I said earlier, I think these two are inevitably married together for substantive reasons.

MR. BORENE: I apologize. It's actually – now, it is 3:00 and I need to wrap it up. But I want to thank all of you, as the audience, for joining us today. We're people who, obviously, here are passionate about this as an issue and making this more effective and responsive for national security and our competitive advantage as a nation.

And I'd like to thank Mr. Butler and our distinguished panel. And for those of you who think that this is a good kind of a program to have this roundtable and you'd like to work with us to continue to do this, I just want to also thank the LexisNexis team and if somebody's a member – any members of the LexisNexis team just kind of raise your hand.

And if afterwards, there'll be a round and catch one of us and ask us how we can work together to continue this line of discussion. And also, I have a note from Mr. Butler that some of the panelists will stick around. So hopefully, you'll join us and we'll continue having those conversations that lead to the kind of innovation that meet these needs we talked about today, I'd very much appreciate it. And thank you to the press club for the venue. (Applause.)

(END)