LAPD-LINCT INTERNATIONAL COUNTER-TERRORISM CONFERENCE

June 5-7, 2013

Los Angeles Police Department
Leadership in Counter-Terrorism (LinCT)

Sponsorship for the conference was generously provided by:

Raytheon

Palantir

Conference Proceedings

Los Angeles, California – June 5-7, 2013

Hosted By

The Los Angeles Police Department

ACKNOWLEDGEMENTS

The LinCT organization would like to extend special recognition to the following organizations for their support of the 2013 LinCT Conference.

Los Angeles Police Department, Counter-Terrorism and Special Operations Bureau
Thank you to the entire Counter-Terrorism and Special Operations Bureau for the detailed and extensive work done to plan and host the conference. We would like to extend a special acknowledgement to Deputy Chief Michael Downing and Lieutenant Anita McKeown for their leadership that made for such a successful and productive event.

The LinCT Tactical Demonstration was sponsored by Universal Services of America. Thank you to their team and the LAPD for demonstrating the top notch response capabilities in true Hollywood fashion.

The Conference Proceedings were developed with staff support from Lafayette Group and the National Consortium for Advanced Policing.

Photography was provided by the Los Angeles Police Department.

Table of Contents

LinCT Alumni Association President's Welcome

I have had the privilege serving as the President of the Leadership in Counter Terrorism Alumni Association (LinCT AA) for the past twelve months. On behalf of the Alumni Association and our partner, the Los Angeles Police Department (LAPD), I would like to present these Conference Proceedings from the 2013 LAPD-LINCT Counter Terrorism Conference. As always, we listened to great speakers and presentations that provided myriad perspectives from the private and public sectors. In keeping with tradition, this proceedings document only captures the LinCT AA meeting portion of the conference.

We approached the planning of this conference differently this year. We had the distinct honor of combining our meeting with the United States National Homeland Security Association (NHSA) conference for a total of five days. The NHSA is a conference held annually in the United States in major urban areas to foster information sharing in all homeland security disciplines. This was a unique and valuable experience for the other Five Eyes partners of Australia, Canada, New Zealand, and the United Kingdom to get a glimpse at U.S. homeland security efforts and to network with specialists from across the nation. This cooperation also was keeping with the theme of this year's conference – building relationships domestically and abroad.

The LinCT AA maintains an invaluable relationship with LAPD, and once again, owes a huge thank you to Deputy Chief Mike Downing and his team for a great meeting and amazing demonstrations. I look forward to seeing everyone again next year for the LinCT meeting in the great city of Los Angeles.

Jon Boutcher
Assistant Chief Constable
Joint Protective Services
United Kingdom
President 2012/13

Leadership in Counter Terrorism Alumni Association
Host Agency Welcome

The threat we face as law enforcement counter-terrorism officials is ever changing and evolving, so we must as well. We cannot succeed without each other domestically and abroad. The Leadership in Counter Terrorism Alumni Association makes it possible for us to continually meet and explore new methods to counter violence. This year, our partnership with the United States' National Homeland Security Association's annual conference enables our peers from the Five Eyes to get a broader perspective of homeland security in the United States. Roughly 1,200 members of the homeland security community gathered to share best practices and lessons learned.

The theme of this year's conference was building relationships domestically and abroad. Presenters discussed the importance of collaboration and collocation of resources. They also explored how the private and public sectors can better work together.

I would like to thank the Counter-Terrorism and Special Operations Bureau for their hard work and attention to detail. Without them, this conference would not be possible. The staff did an excellent job coordinating the conference and demonstrations. We look forward to being able to support and play host to the conference into the future.

Sincerely,
Michael P. Downing
Commanding Officer, LAPD Counter-Terrorism and Special Operations Bureau
Past President, Leadership in Counter Terrorism Alumni Association (2010-2011)

Host Agency Profile: Los Angeles Police Department Counter-Terrorism and Special Operations Bureau

The Counter-Terrorism and Special Operations Bureau (CTSOB) is responsible for planning, response, and intelligence activities related to terrorism and other crimes. CTSOB's mission is: "To Prevent terrorism by effectively sharing information aimed at disrupting terrorist's operational capability and addressing the underlying causes associated with the motivational component; to Protect the public and critical infrastructure by leveraging private sector resources and hardening targets; to Pursue terrorists and those criminal enterprises that support them; and, to Prepare the citizenry and the city government for consequences associated with terrorist operations against the city."

Deputy Chief Michael Downing is the Commanding Officer of CTSOB. CTSOB is comprised of the Major Crimes Division (MCD), the Emergency Services Division (ESD), Metropolitan Division, Air Support Division (ASD), and Emergency Operations Division (EOD).

The Major Crime Division's primary objective is the prevention of significant disruptions of public order in the City of Los Angeles. MCD investigates individuals or groups who plan, threaten, finance, aid, abet, attempt, or perform unlawful acts which threaten public safety. MCD investigators are committed to preventing individuals or groups from harassing or harming others on the basis of race, religion, national origin, or sexual orientation. The division's Commanding Officer is Captain Steven S. Sambar. MCD sections include:

- Criminal Conspiracy Section
- Anti-Terrorism Intelligence Section
- Liaison Section
- Organized Crime Section
- Surveillance Support Section
- Source Development Unit
- Criminal Investigative Section
- Analysis Section
- Joint Regional Intelligence Center

The Emergency Services Division is charged with safeguarding the public by preventing and/or mitigating terrorist and other criminal activities through threat assessments, detection, deterrence, and the rapid response to criminal incidents. The division's Commanding Officer is Captain Thomas McDonald and its sections include:

- Archangel Section
  - Critical Asset Assessment Team
  - R&D Training Unit
  - Advanced Technology Unit
  - Asset Protection Cadre
- Hazardous Devices/Materials Section
  - Bomb Squad Unit
  - Hazardous Materials Unit
- Bomb Detection K-9 Section
  - Bomb Detection K-9 Unit

Leadership in Counter Terrorism Overview

The following is a brief overview of the LinCT program and its history:

- LinCT was initiated in 2004 as a joint leadership project between the Federal Bureau of Investigation (FBI), Scottish Police College, the Police Service of Northern Ireland, The Royal Canadian Mounted Police, Harvard University and St. Andrews University;
- Focus is on the prevention of terrorism;
- There are three primary threads of content that are integrated throughout the program: Counter Terrorism, Intelligence and Leadership;
- The program is primarily strategic rather than operational;
- The critical outcomes are to improve inter-agency cooperation through enhanced communications, information sharing and personal relationships;
- In 2006 the program was expanded to the Pacific Region in partnership with the Australian Federal Police and the Australian Institute of Police Management;
- Participants represent the partner countries' domestic and Federal Law Enforcement, Military, and Intelligence Communities; and
- The LinCT program is governed by an international Board of Governors consisting of the Chief Executive Officers from the participating countries' lead agencies.

2013 LAPD-LINCT International Counter-Terrorism Conference Theme: Collabortation

The world is changing rapidly. With the birth of the Internet, criminal and terrorist organizations have globalized their operations. In response, law enforcement must continue to do so as well. This can only be accomplished by building relationships and partnerships at home and abroad. The Leadership in Counter Terrorism Alumni Association (LinCT AA) not only took this opportunity to continue its partnership with the Los Angeles Police Department (LAPD), but also increased its reach and partnered with the United States National Homeland Security Association (NHSA) conference. The NHSA holds a conference annually in the United States in major urban areas to foster information sharing in all homeland security disciplines. This partnership increased the LinCT AA's reach and ability to build partnerships around the world. To highlight the importance of this, the theme of the conference was collaboration. To be successful, many speakers presented overlapping themes that are tried methods of building partnerships that are effective and last as discussed in the textbox below.

2013 LinCT Conference Themes:

While all panelists discussed the importance of collaboration, there were also some major topical themes:

Building Partnerships

Conducting Exercises and Training

Countering Violence Extremism

Embracing Social Media

Enhancing Cyber Capabilities

Ensuring Global Information Exchange

Performing Risk-Based Security

The remainder of this section provides an overview of each of the themes as they were presented by panelists. Each theme is followed by a list of ideas on how to better achieve these strategic objectives. The intent is that these lists will help conference participants continue to be innovative in these areas over the coming year.

Building Partnerships

The LinCT Association and the annual conference are always about finding opportunities where alumni can work together. The panelists this year stressed the importance of building partnerships at all levels of law enforcement as well as outside the law enforcement community. With the limited resources, law enforcement must leverage every asset it can. This requires not only building the relationships and partnerships, but also solidifying and institutionalizing them throughout organizations. The following opportunities for building partnerships to improve policing practices were mentioned by panelists:

- Failing to establish relationships, both domestically and internationally, is the greatest threat to the United States.
- Working together, the international community will continue to be able to more effectively combat an evolving threat through great partnerships.
- Awareness and good relationships at the local level will often be the difference between averting and experiencing an attack.
- Working with various communities and first responders is imperative to ensure a smooth, safe special event.
- Conducting investigations in foreign countries can be challenging so ensuring partnerships and relationships are in place ahead of time is imperative.
- Increase collaboration internationally to detect and prevent people from traveling to and from terrorist conflict zones.
- Create partnerships nationally and internationally to increase information sharing and preventative efforts.
- Working together and sharing information is the only way to combat a global threat.
- Collocation of intelligence and law enforcement is imperative to foster information sharing and institutionalize relationships within an organization rather than relying on personally developed relationships.
- Engage victim assistance organizations to understand from a victim's perspective how to improve response.
- Build partnerships between the public and private sector and come together to solve identified problems that result in structural changes.
- Engage the community to develop counter messaging and respond to the threat with the strength of the community.
- Engage the community in a language they understand and utilize in real time.

Conducting Exercises and Training

LinCT participating nations and individuals are continuing to find new strategies to improve their processes. Conducting exercises and training is a critical step for testing and institutionalizing these approaches and is imperative to ensure incidents and events go as smoothly as planned. These engagements also serve as opportunities to build and strengthen partnerships that must already be in place before an incident occurs. For instance, the panelists discussed the following:

- Exercise and train regularly to solidify relationships and roles because waiting until conflict is too late.
- Increase awareness of vulnerabilities and improve processes by exercising and training together.
- Test and exercise to be more aware of weaknesses and needed improvements.
- Include victim assistance organizations in exercises and training to ensure smooth operations at the time of an incident.
- Invest in exercising and training to build and enhance relationships, which are essential to successful special events.
- Engage communities, listen to their needs, and understand their concerns as homeland security is not just a law enforcement problem.
- Include private sector in training and exercises to better prepare for an incident.

Countering Violent Extremism

The terrorist threat is ever changing and panelists highlighted the evolution of the threat, where it stands today, and how it will shift in the future. As all nations progress into countering violent extremism, it is becoming clear all efforts must ensure civil rights and civil liberties are upheld. Some suggested strategies included:

- Adapt to the ever evolving violent extremist threat.
- Strike a balance between monitoring persons of interest and protecting civil liberties and civil rights requires a wide-ranging, multi-dimensional whole of government approach.
- Engage communities, listen to their needs, and understand their concerns as homeland security is not just a law enforcement problem.
- Share information with the community and engage community leaders to develop counter narrative messaging strategies.
- Evolve with the threat to counteract violent extremism.

Embracing Social Media

Law enforcement is slowly embracing social media to enhance community engagement as well as to support investigations. Social media has helped make it possible for criminal enterprises to have a global reach in a language that is understood by the younger generations. The following were presented by panelists as ways to continue to integrate social media into community engagement strategies and support investigations:

- Utilize social media to mobilize the community and correct misinformation.
- Monitor social media during a crisis to get real time information from hostages and witnesses.
- Even the playing field with terrorist organizations and transition into the digital age.
- Embrace social media and be creative with counter messaging as al Qaeda and others already have.
- Utilize the information placed on the Internet to enhance and support investigations.

Enhancing Cyber Capabilities

With the birth of the Internet, criminal and terrorist organizations have globalized their reach. They can attack a country without ever stepping foot on its soil. They can attack a corporation without ever stepping foot into the headquarters. This threat is ever changing making international partnerships even more important and vital to combatting these organizations and their activities. Specific strategies included:

- Improve legislation to ensure civil liberties and civil rights are protected when enhancing cyber capabilities.
- Enhancing cyber capabilities is imperative to protect critical infrastructure.
- Generate discussion on legislation and boundaries needed to investigate cyber crimes while protecting civil liberties and civil rights.
- Train and educate all levels of employees that have access to systems vulnerable to attack.
- Enhance capabilities to ensure social media can be used and is reliable.

Ensuring Global Information Exchange

The global community we live in today is just as accessible to criminal organizations and their activities. The Internet allows for criminals to attack a country without even stepping foot inside its borders. Generating and maintaining international partnerships and relationships has become vital to preventing and combatting these criminal elements. Open communication is integral to these partnerships being able to fully understand the global picture of criminal and terrorist organizations. The following were suggested as opportunities for continuing to ensure the exchange of information globally:

- Reach out to international partners to bolster domestic efforts.
- Coordinating and collaborating globally is crucial to understanding the evolving threat.
- Work with past and future special events hosts to learn and plan for the future.
- Execute international investigation as the birth of the Internet has resulted in a transnational threat.
- Deploy liaisons to private sector incidents and vice versa to ensure information flow.
- Share information and collaborate on operations internationally to continue to successfully combat terrorism.
- Amend legislation to allow for international investigations.
- Share information globally as the threat is ever changing and evolving.

Performing Risk-Based Security

At all levels of government, agencies are trying to find ways to do more with less. An ideal way to deal with budget cuts is to funnel resources to the protection of the most likely targets. By doing so, law enforcement is increasing its chance of preventing an attack. The following ideas are ways to best allocate resources:

- Employ risk-based security methods tailored to the evolving threat.
- Conduct cost-benefit analysis of threats and protective efforts by enlisting and empowering the private sector and engaging the community.
- Assess the biggest risks and vulnerabilities to ensure targeted security as a country can never be 100% secure.
- Discuss risk-based security principles with senior executives because this is language they are familiar with and employ risk-based security to minimize disruptions affecting the bottom line.

Keynote Speakers

Lieutenant General Michael Flynn, Director, Defense Intelligence Agency

Collaboration: Keynote

Building Partnerships: Failing to establish relationships, both domestically and internationally, is the greatest threat to the United States.

Conducting Exercises and Training: Exercise and train regularly to solidify relationships and roles because waiting until conflict is too late.

Enhancing Cyber Capabilities: Improve legislation to ensure civil liberties and civil rights are protected when enhancing cyber capabilities.

Ensuring Global Information Exchange: Reach out to international partners to bolster domestic efforts.

The Defense Intelligence Agency (DIA) provides intelligence support to the U.S. military and is one of the largest technology and science agencies in the world. The Director, Lt. General Flynn, discussed the importance of developing partnerships to aid needed change.

Today, the United States is in a profound transition phase. The country is winding down direct combat engagements and is recovering from economic uncertainty, both of which affect our

national security policies. We are at a point in time where we need to change our thinking and way of doing things by first understanding our strengths and weaknesses. The greatest threat to our country comes if we do not work together, whether it is with our foreign partners or our local law enforcement. On the flip side, the United States' biggest strategic advantage is our strong rule of law, so we need to continue the charge to protect and strengthen it over time. Being successful through this transition will require us to develop partnerships, understand the operational environment, think long-term, evolve with changing communications, and address cyber threats.

We need to ensure operations and intelligence personnel are blended and work together; trust will be the key in building these into cooperative relationships. Therefore, it is imperative to exercise and plan together rather than try to build relationships at the time of the conflict.

The Arab awakening is captivating the world. We need to understand the culture as we would understand our neighbor, which will lead us to a greater understanding of the operational environment. A recent study commissioned by the Chairman of the Joint Chiefs of Staff looked at the last ten years of war and found the number one lesson learned was the "failure to understand the operational environment in which we were operating in," which led to a mismatch of resources. Local law enforcement succeeds because officers grow up in the cities and cultures they police, which allows for more effective policing. We need to exploit this expertise.

We have to think long-term to build a foundation and create a framework for years to come. Understanding global trends will help us predict needs. For instance, India is projected to grow by another 600 million people in the next 20 years, which will surpass China's population. This will cause tension to create jobs and develop resources for that number of people. Additionally, global communication is changing. The continent of Africa is rapidly becoming a global communicator as cellphones have become more widely used. Now, the continent comprises 47% of the global cellphone market. Asia is now dominates Internet usage, which is just another one of the global communication trends that is providing a "voice to the voiceless." Impoverished areas now have the ability to share their tragedies and injustices as evident by the Middle East catapulting their tragedies into the global media.

With the birth of the Internet came a new threat – cyber crime. We must make decisions when fighting this invisible war on how to move forward and still protect privacy. Legislation has not caught up with this threat, resulting in problems with crossing the line that has been there to maintain the freedoms and liberties we cherish.

Natural resources will eventually become sparse. For instance, obtaining fresh water will become a challenge and an issue of national security. The three largest fresh water supplies are located in Africa, the United States, and the Himalayas but two of those areas are difficult to even access. It is imperative to start planning now and put infrastructure and relationships in place to do so in the future. This demonstrates the need to shift our way of thinking in order to

determine what is important to our economy. We have focused on protecting oil in the Middle East, but as other regions gain influence and a voice and resources deplete, our focus will shift.

> ***"Fusion is not a word. It is a way to think."***
>
> *- Lt. Gen. Michael Flynn*

We cannot be stuck in yesterday and need to look for new ways to change and adapt for tomorrow. We are being threatened differently. We must be intellectually curious to survive. Transnational organized crime is intersecting with terrorist organizations. Therefore, our resources, priorities, collaboration, and partnerships need to change.

In closing, the Director shared some professional lessons learned to aid in this transition:

- Hold people accountable and make them responsible to build a sense of ownership
- Decentralized decision making requires an increase in situational awareness
- Leaders need to be efficient with resources and priorities
- Maximize integration and transparency to build trust

John Pistole, Administrator, Transportation Security Administration

Collaboration: Keynote

Building Partnerships: Working together, the international community will continue to be able to more effectively combat an evolving threat through great partnerships.

Conducting Exercises and Training: Increase awareness of vulnerabilities and improve processes by exercising and training together.

Countering Violence Extremism: Adapt to the ever evolving violent extremist threat.

Ensuring Global Information Exchange: Coordinating and collaborating globally is crucial to understanding the evolving threat.

Performing Risk-Based Security: Employ risk-based security methods tailored to the evolving threat.

Mr. John Pistole is the current and fifth Administrator for the U.S. Transportation Security Administration (TSA) that oversees U.S. airports, highways, railroads, ports, mass transit systems, and pipelines. He provided the keynote address on the second day and discussed TSA's role in homeland security. The United States has 275 airports with non-stop international service, not to mention the large number of cargo planes arriving daily from overseas, so it is

imperative to work with international counterparts in exercises, training, and transportation protocol development.

Over the last 25 years, there have been numerous transportation attacks and plots. However, the methods of attack are constantly and quickly evolving. Terrorists are using the same bomb makers, but they have demonstrated a great ability to adapt and beat our current security measures. Therefore, as law enforcement, we have to adapt to threats as the terrorists do. For instance, in recent years there has been an increase in the use of non-metallic IEDs that cannot be detected with metal detectors (e.g., the underwear bomber and the Yemen cargo plane incident). Even though they were unsuccessful, they have cost us billions of dollars in security improvements after the fact. International collaboration is crucial to understand the evolution of the threat and plan ahead.

To help combat the evolving threat, TSA is transitioning to a risk-based approach and using its Intermodal Security Training Exercise Program (I-STEP) to increase its ability to prepare for and respond to an incident "by increasing awareness, improving processes, creating partnerships, and delivering transportation-sector network security training exercises." TSA is using and encourages law enforcement to use I-STEP to assess vulnerabilities and appropriate responses. Terrorists focus on certain types of targets and so should we. After interviewing captured terrorists, we have learned that the three biggest deterrents for an attack are uniformed officers, K-9s, and closed circuit television (the latter does not apply to suicide bombers). Therefore, we need to prioritize our critical infrastructure and put deterrent measures in place, not to mention ensure there will be a coordinated response. The best way to ensure a coordinated response effort is to conduct exercises ahead of time to test we are up and running in the most efficient and effective manner possible. These steps put together will also help to get back to normal as quickly as possible after an attack and to prevent the fear and economic damage terrorists also desire.

TSA's risk-based approach will have direct advantages for airports, especially considering the agency's need to screen 630 million people a year in airports. By implementing the TSA Pre✓™ program, certain, pre-qualified, low-risk persons will receive expedited screening benefits if they pass an application process and background check. Travelers over the age of 75 and under the age of 12 are good groups for inclusion in this program since they do not generally pose a threat. These approved travelers have separate screening lanes that allow them to leave on "shoes, light outerwear, and belts, as well as leaving laptops and 3-1-1 compliant liquids in carry-on bags." The goal is to get to the point where 25% of public travelers go through expedited travel.

The international community will continue to be able to more effectively combat an evolving threat through great partnerships and risk-based security measures, such as the TSA Pre✓™ and I-STEP.

Honorable Michael Chertoff, Former Secretary U.S. Department of Homeland Security and Chairman and Co-Founder, The Chertoff Group

Collaboration: Keynote

Building Partnerships: Awareness and good relationships at the local level will often be the difference between averting and experiencing an attack.

Conducting Exercises and Training: Test and exercise to be more aware of weaknesses and needed improvements.

Embracing Social Media: Utilize social media to mobilize the community and correct misinformation.

Enhancing Cyber Capabilities: Enhancing cyber capabilities is imperative to protect critical infrastructure.

Performing Risk-Based Security: Conduct cost-benefit analysis of threats and protective efforts by enlisting and empowering the private sector and engaging the community.

Michael Chertoff, the former Secretary of the U.S. Department of Homeland Security, provided the keynote address on the second day. He views homeland security as an all-hazards business even though the media tends to focus on just one of four all-hazard areas – terrorism. The current threat environment encompasses four areas: physical security, criminal/transnational

groups that leverage modern technology to be more efficient, cyber security (recently designated as the number one threat to the United States because this encapsulates transportation and physical risks), and terrorism. Dealing with these four threats, we need to employ a holistic approach encompassing prevention, reduction of vulnerabilities in the community, and effective response.

Threats today have transformed themselves; therefore, law enforcement must transform as well. The focus must shift to more emphasis on local law enforcement's ability to get information, understand it, and respond. Engaging the community plays a significant role in this effort; therefore, employing programs such as "See Something, Say Something" and social media become increasingly important at the local level. Awareness and good relationships at the local level will often be the difference between averting and experiencing an attack.

Social media is also an important consideration in incident response. It can cause problems because of how easily it allows for the spread of misinformation. However, it can be used positively to mobilize the community and correct misinformation. Therefore, law enforcement needs to embrace social media and have a plan to utilize in emergencies, including both natural disasters and acts of terrorism. "If you ignore social media, it will become an obstacle. However, if you elicit social media, it becomes an ally."

> ***"If you ignore social media, it will become an obstacle. However, if you elicit social media, it becomes an ally."***
>
> *- Michael Chertoff*

In addition to engaging the community, Secretary Chertoff offers a risk-based management solution to incident prevention and response. It involves a cost-benefit analysis of threats and protective efforts, enlisting and empowering the private sector, and engaging the community. The basic strategy involves seven stages.

1) Identify the threats – We need to understand the threat and have information put into context as soon as possible to weigh options.
2) Assess the threat and your vulnerabilities – We need to understand where our points of danger are located.
3) Prioritize where to protect – We cannot protect everything and be everywhere, so we must weigh the consequences.
4) Invest in protection – Even in a time of budget cuts, we need to have the resources available to protect the public.
5) Test and exercise what we have invested in – We will not know our weaknesses unless we test our investments and our planning protocols.

6) Monitor the continuously evolving threat – It is always evolving, so we must change with it.
7) Apply lessons learned – We must not focus on whose fault it was, but rather what we learned from it. We learn from failure, not from success.

All of these approaches need to be considered in the context of the evolving al Qaeda threat. They are moving away from large-scaled attacks to smaller, more frequent attacks, which are harder to detect and analyze because each attack is tailored to a specific location. Also, there has been an increase in safe havens for al Qaeda operatives. Additionally, the upheaval in North Africa has strengthened al Qaeda affiliates in the region.

In closing, threats today, such as North Korea and Iran, do not use "our rule book;" therefore, what they cannot or do not develop, they will buy to attack our critical infrastructure. Most of our critical infrastructure is in the hands of private companies. Therefore, the burden falls on local law enforcement to protect us. Critical infrastructure owners and operators must be vigilant about checking for cyber security breaches while local law enforcement must know the vulnerabilities of their area's critical infrastructure in the event it is compromised. This includes knowing how communications might be affected and the confusion and misinformation that will result. This can only be done by being prepared through training and exercises.

Keynote Special Briefings

2012 London Summer Olympic and Paralympic Games – Assistant Commissioner Chris Allison, London Metropolitan Police Service

Collaboration: 2012 London Summer Olympics

Building Partnerships: Working with various communities and first responders is imperative to ensure a smooth, safe special event.

Conducting Exercises and Training: Invest in exercising and training to build and enhance relationships, which are essential to successful special events.

Ensuring Global Information Exchange: Work with past and future special events hosts to learn and plan for the future.

The 2012 London Summer Olympics was a tremendous success, thanks to the planning, training and exercising that preceded the games. From the lighting of the torch to the closing of the Olympic Village, the operation lasted 121 days. It involved 12 police areas and all 54 police departments throughout the United Kingdom. There were 34 venues, an estimated 800,000 visitors using public transportation on the busiest day, and 137 "protected persons" attending events. Even with all these security concerns, it was essential to make this a "sporting event with a security overlay, not a security event in which a sport was to be played." Also, so as not to distract from the games, it was imperative that all security should have the same "look and feel" throughout the United Kingdom to elicit the same level of comfort for the athletes and visitors. To ensure the best operation possible, the law enforcement elements planned and trained at the "severe" threat level (second highest) even though the actual threat level was

lower at "substantial." Finally, it was essential to keep it a "blue" event by having the streets of policed by the British Police Services and not the military.

There were four areas of risk: terrorist activity; criminal activity, including serious and organized crime; public protest and domestic extremism; and non-malicious hazards (e.g., pandemic, heat wave).

> ***"If logistics don't work, the operation won't."***
>
> *– Assistant Commissioner Chris Allison*

While the British Police Services drew upon many established resources, there were a few initiatives created just for the Olympics.

1. The National Olympic Coordinator position charged with coordinating, planning, leading, and delivering the national response.
2. The National Olympic Coordination Center was built to support the Coordinator with 17 different organizations represented to allow for seamless information sharing.
3. The Olympic Intelligence Center started three years before the event to house all criminal and counter-terrorism intelligence agencies, which are normally kept separate. It produced products for the Coordinator and Olympic sponsor agencies on a daily or hourly basis as needed.
4. The Protection Coordination Office looked after the 137 protected individuals. This was three times the number of people the United Kingdom had ever protected at one event.
5. The International Liaison Unit was established to communicate with the 205 participating countries to ensure the safety of their athletes. This unit also provided information to countries that will be hosting the Olympics in the future to share best practices and lessons learned.
6. The Operation Podium was the designated response unit to serious and organized crime concerns, such as fraud and counterfeit tickets.
7. The Community Engagement Team ensured coordinated messages were given throughout the country.

The most important takeaway was the need for testing and exercising; event planners cannot invest enough time and money in exercising. This assists with establishing relationships and preparedness in advance of a disaster to allow for smoother and more seamless operations during an actual event. However, large scale events always have unforeseen circumstances, so expect the unexpected. During planning, the United Kingdom contracted with a private security firm to provide 5,000 military personnel. But, a year out, the firm realized it underestimated its needs by 13,000. The UK military planned to provide an additional 7,000. However, two weeks prior to the Games, the private security company failed to deliver the original 5,000, so the military and the UK Police Services had to provide the additional personnel. Overall though, it was a huge success.

Hostage Crisis Near In Amenas, Algeria – Detective Superintendent Jim Stokley, London Metropolitan Police Service

Collaboration: Hostage Crisis Near In Amenas, Algeria

Building Partnerships: Conducting investigations in foreign countries can be challenging so ensuring partnerships and relationships are in place ahead of time is imperative.

Embracing Social Media: Monitor social media during a crisis to get real time information from hostages and witnesses.

Ensuring Global Information Exchange: Deploy liaisons to private sector incidents and vice versa to ensure information flow.

On January 16, 2013, a group of al Qaeda-linked terrorists affiliated with Mokhtar Belmokhtar took 800 people hostage at the British Petroleum (BP) Tigantourine oil and gas facility near In Amenas, Algeria. At least 39 people from nine countries lost their lives over a four day period. Because the facility is owned by a London-based company, the London Metropolitan Police was charged with heading up the operations and investigation.

In an event of this magnitude, it is imperative to communicate and get the correct information out as soon as possible. To assist with this process, the London Metropolitan Police Service created a fusion cell to begin monitoring Facebook, Twitter, and media outlets to get a sense of what they were dealing with from the perspective of hostages. Regularly scheduled briefings were set up for the command staff, which was extremely helpful because it allowed time to oversee the investigation and not spend all of the time fielding questions. Command staff knew precisely when they would receive an update.

In addition to communication challenges, this incident was both a terrorist attack and a hostage situation simultaneously. Each required a different response and posed different problems. Addressing both together while still meeting the needs of each required a variety of response efforts, some of which were used for the first time.

The hostage negotiators set up 30 Red Centers across the United Kingdom to facilitate communication with the families that were in contact with hostages and terrorists, so this allowed negotiators easy access. As it was apparent more hostages would likely be killed, family liaison officers were deployed to the Red Centers to provide support to the families

victims. This was the first time they had done this, but it served as a continuing comfort to the family rather than transitioning to the family liaison officer only upon the death of a love one.

Another problem was identifying who the hostages were and where they were located because the gas and oil fields are a joint venture of multiple companies and subcontractors. The London Metropolitan Police Service deployed officers to all the companies' human resources departments to identify the employees onsite. BP also has their own crisis center, so London Metropolitan Police Service officers were deployed there and directly to the gas and oil fields along with Federal Bureau of Investigation agents to assist with identification and response. This was very helpful to have familiar law enforcement specialists at the scene even though they were in a foreign country. The officers deployed included forensic and victim identification specialists, hostage negotiators, and investigators.

When working with BP, it was important to have a BP liaison assigned to the investigation to deal with private industry issues out of the realm of law enforcement expertise, especially when it comes to decisions and logistics related to the oil and gas industry.

As discussed throughout the conference, social media played a large role. Witnesses and hostages sent pictures to the press and their families. The London Metropolitan Police Service was able to use those pictures and information to handle the hostage situation as well as share the information with their Five Eyes partners that were involved (United States and Canada) in daily briefings at the Canadian Embassy. However, social media did cause a potentially threatening problem. Terrorists wanted the publicity and access to western news agencies, which they got. But, the police had to work with media to prevent them from identifying where hostages were hiding because terrorists were monitoring the news.

Conducting an investigation involving a terrorist attack and hostages required a delicate balance. As hostages escaped, they sustained mental and physical injuries as they were beaten and had to watch the execution of other hostages. Therefore, investigators had to ensure the hostages received the proper medical treatment while still getting as much information as possible because the incident was ongoing. Additionally, investigators needed to gather forensic evidence from clothing and other items, and doing so became tricky while still trying to address the mental and physical health of the victims.

The Gatwick Airport located just south of London played an important role because it shut down a gate for three weeks to allow all flights from Algeria to enter through one gate at one airport rather than at various entry points across the country. This was beneficial for many reasons. The gate acted as a triage center allowing for all evidence collection and processing to occur at one point. They were also able to take statements, collect cell phones and clothing, and treat hostages all at one point. Additionally, no media was permitted access to the gate so families were able to have privacy as their loved ones returned.

Finally, when attempting to conduct an investigation in another country, there will be some political challenges. It was difficult to get permission from the Algerian government to conduct an investigation and hostage rescue. This caused problems with identification of body parts and victims. Initial identification of body parts was done by the Algerians by nationality of the victims, so many body parts were misidentified. The investigators had to create a proper identification process, approved by all nine countries involved in the investigation, to ensure the return of remains to the correct country. This highlights important it is to have international relationships in place prior to an incident.

Panel Overviews

Day1, Panel 1 – Current Threats, Issues and Responses – a "Five Eyes" Review

- Moderator – **Jon Boutcher**, Assistant Chief Constable, Hertfordshire Constabulary
- **Michael Downing**, Deputy Chief, Los Angeles Police Department
- **Mike Richards**, Deputy Director, New Zealand Security Intelligence Service
- **John Noble**, British Embassy, Washington, D.C.
- **Stuart Thorn**, Deputy Director General, Australian Security Intelligence Organization
- **Michael Pierce**, Assistant Deputy Director, Canadian Security Intelligence Service
- **Michael Leiter**, Senior Counselor to CEO, Palantir Technologies

Collaboration: Current Threats, Issues and Responses

Building Partnerships: Increase collaboration internationally to detect and prevent people from traveling to and from terrorist conflict zones.

Countering Violence Extremism: Strike a balance between monitoring persons of interest and protecting civil liberties and civil rights requires a wide-ranging, multi-dimensional whole of government approach.

Ensuring Global Information Exchange: Share information and collaborate on operations internationally to continue to successfully combat terrorism.

The Five Eyes partners presented on their individual threat as well as their global perspective. Generally, all five countries are affected by the upheaval in the Middle East and feel its effects at home. This is in turn causing a "travel problem," because citizens going to Syria to fight and returning home with "street credibility" aiding in recruitment of other as well as increasing the likelihood of an attack at home. Together, the Five Eyes must continue to share information and collaborate on operations to continue to successfully combat terrorism.

<u>New Zealand</u>

In New Zealand, the number one counter-terrorism threat is still Islamic extremism even though it is rated low. The majority of challenges derive from a small number of Somali immigrants entering in the mid-1990s as well as from some converts to Islam. Since 2000, a large number of those Somalis have immigrated to Australia from New Zealand. There are no radical Imams or survivors of Middle East conflict zones yet in New Zealand. A non-Islamic

threat faced by both Australia and New Zealand comes from becoming a safe haven for dissidents. There is a concern this may cause these countries to be at a greater risk for acts of violence.

Al Qaeda narrative is still a powerful driver, and the decentralization of the organization has ensured its longevity. The Internet fosters easy access to vulnerable people to aid in radicalization. Additionally, the continued presence of jihadi conflict zones provides those with the motivation to fight the opportunity to do so. Those that survive conflicts and return to home countries may pose a great threat and raise risk of extremist action in New Zealand.

Monitoring individuals requires a tough balance. It is hard to know when a person of interest is no longer a concern or to know when someone crosses from expressing attitudes of extremism to advocating extremism. Striking a balance between monitoring persons of interest and seeking assistance from our partners becomes increasingly difficult as countries have the responsibility to protect their own citizens while having a competing responsibility to protect human rights both at home and internationally throughout investigations and aiding international partners.

An effective response must be wide-ranging, multi-dimensional, and involve the whole of government. Additionally, we must actively interact with the community and religious leaders. This encourages open and frank dialogue that helps to prevent and combat extremism.

United Kingdom

The threat is by no means over. Below are five reasons to still be concerned today; therefore, efforts must not be relaxed:

1. The brutal murder of a British soldier on May 22, 2013, as well as the attempted murder of the first responders to the incident. The concern becomes how to stop an attack that involves relatively few people.
2. Six extremists are due to be sentenced for planning an attack on a right wing rally in the North of England.
3. The overall number of investigations and persons of interest have not reduced. Everyday this requires tough decisions regarding which target to follow and which not to follow as we cannot monitor all of them.
4. Certain events around the world, such as the Syrian civil war and South Asia post drawdown in Afghanistan.
5. Technology is present and available to terrorists.

Even though the threat is still present, there should be a reflection on the positive outcomes of recent events. The following are five reasons to be more positive and remember a difference has been made:

1. The United States' impact on al Qaeda completely changed the threat we are facing.

2. The United Kingdom's success for preventing and prosecuting attempted acts of terror. On April 13, 2013, 11 men were sentenced for their planned attack involving mass casualties with a projected larger impact than the London subway attack.
3. We are able to generate intelligence to disrupt planned terrorist attacks.
4. The United Kingdom's transformation to a collaborative effort between intelligence and police forces.
5. International relationships that allows intelligence to flow in all directions between the Five Eyes partners.

Australia

The primary focus in Australia is on Islamist extremism. Recent thwarted plots have involved critical infrastructure, mass gatherings, and military facilities. Also, they have seen an increase in radicalization through the use of the Internet, including through the online magazine *Inspire*. Recent domestic investigations have been related to the events in Syria. Citizens are traveling to Syria to join the fight with the opposition and they are going to Afghanistan and Pakistan to receive training. This also raises the concern for when citizens return to Australia whether they will bring the fight home.

Also, there are long standing links to Hezbollah in Australia within the strong Lebanese community. There has been fundraising among the strong support base but no attempted planning or preparations for an attack. Resources have been increased to monitor this issue.

A final concern is the release of the Bali bombers into the community upon completion of their sentences in the next couple of years.

Canada

Domestic terrorism is the number one threat in Canada, but it is followed by concerns of cyber attacks, economic espionage, and weapons of mass destruction. Specific to the domestic terrorist threat, al Qaeda Sunni Islamic extremists are the main concern in Canada followed closely by domestic radicalization, which has resulted in many arrests. Additionally, Canada has right- and left- wing extremists who have set off explosives, but they are not a major concern. Lone wolf attacks are also a concern and an alarming problem because they are so hard to detect. Finally, Hezbollah is of concern because of recent issues Canada has had with Iran. But, this is not a high risk yet.

In Canada, the majority of persons of concern are 21-35 years of age and have connections to one another through high school. Most are employed and almost half have a post-secondary education. This is different from European partners who report persons of interest as poor and disenfranchised. The only time Canadian persons of interest fit the same profile as European, poor and disenfranchised, is in the Canadian Somali population. Persons of interest take part in the typical terrorist activities, such as eliciting finances, conducting attacks, recruiting and radicalizing, and training.

An emerging problem is the "traveler problem." With the increase in technology and the ability to travel so easily, there is problem with citizens leaving the country to receive training abroad and fight in overseas conflicts. This is not new and stems back to the 1980s. The civil war in Syria has revitalized the problem and is creating an international dilemma.
The decentralization of al Qaeda is a big driver to the traveler problem and will only get worse because of how difficult it is to investigate why someone travels to a particular location. A person can easily cover travel to terrorists' hot beds by claiming the trip is to see family, receive religious education, or provide other legitimate reasons backed by a constitutional right to travel. This makes investigations into a person's travel plans very difficult. For example, two Canadians were involved in the attacks at the Algerian oil and gas fields discussed earlier in the conference.

Furthermore, concerns increase when travelers return home with "street credibility" for fighting in conflicts abroad. This aids in recruitment and radicalization of others. This problem is only going to get worse, making it imperative that the Five Eyes need to collaborate and run joint operations, not just share information, to quash the travelers problem.

United States

Overall, the United States has been successful since September 11th in preventing terrorist attacks at home. Only 18 people have been killed in the United States since 2001. Moving forward, the following are five observations to consider.

1. The attack on the Boston Marathon did not present anything surprising aside from the tactical surprise of the event itself. In other words, the way the two men were radicalized, their tactics and techniques, the use of the Internet, and the City's response were all predictable. This is a good thing and should highlight that we have a good sense of how the enemy will operate even though this means we will not stop everything.
2. Counter-terrorism partnerships, aside from ones built in the Five Eyes and other European countries, are in shambles in countries that involve the Arab awakening (e.g., Libya and Egypt). These relationships are either frayed or gone, which limits our insight into threats and puts enormous pressure on us.
3. A weapons of mass destruction (WMD) attack has a low likelihood, however it is still a high consequence threat because the psychological effect of an attack like this, regardless of the fatalities, would rival the trauma seen after September 11th. Great strides have been made against WMDs, so the threat has transitioned from a large device to a smaller device. These small scale devices are hard to detect, especially on the biological front because they are only detectable upon dispersal of the biological agent.
4. The United States spends roughly $100 billion a year on counter-terrorism, which includes the cost of the wars in Iraq and Afghanistan. We have gotten a great return, but we cannot sustain this type of funding; therefore sustaining our capabilities will be a challenge moving forward.

5. Terrorism Fatigue (i.e., complacency among policy makers) will and has occurred because there have not been significant attacks since September 11th. As a result, there will potentially be less pressure to fight al Qaeda in the future. Furthermore, politicians, the public, and the press have gotten so accustomed to things going well that when things go wrong, they turn on the counter-terrorism professionals. This will in turn affect recruiting efforts in the counter-terrorism field moving forward.

Day 1, Panel 2 – The New Threat Landscape, the Limitations and Adaptations into the Future

- Moderator – **Rob Delaney**, First Assistant Director, Attorney General's Department
- **Philip Mudd**, Retired, Central Intelligence Agency, Director Global Risk, Southern Sun Asset Management
- **Celia Mathieson**, Head of Security Services, United Kingdom
- **James Malizia**, Assistant Commissioner, Federal Policing Operations, Royal Canadian Mounted Police
- **Frank Cilluffo**, Director, Homeland Security Policy Institute, George Washington University

Collaboration: New Threat Landscape, the Limitations and Adaptations into the Future

Building Partnerships: Create partnerships nationally and internationally to increase information sharing and preventative efforts.

Countering Violence Extremism: Engage communities, listen to their needs, and understand their concerns as homeland security is not just a law enforcement problem.

Enhancing Cyber Capabilities: Generate discussion on legislation and boundaries needed to investigate cyber crimes while protecting civil liberties and civil rights.

Ensuring Global Information Exchange: Execute international investigation as the birth of the Internet has resulted in a transnational threat.

Performing Risk-Based Security: Assess the biggest risks and vulnerabilities to ensure targeted security as a country can never be 100% secure.

The panel discussed the threat landscape for the future, how it is changing, and ways to adapt. Increasingly, the public expects law enforcement to stop incidents before they happen. The public thinks law enforcement professionals are prevention and security specialists and not solely law enforcement or intelligence specialists. Therefore, law enforcement needs to change its mindset toward prevention.

As a whole, the panel agreed that even with the recent successes, al Qaeda is still a threat, and efforts cannot be eased as they will regain strength. The leadership is still very much intact. In fact, some of the "old school terrorists" who fought in the Balkans and Chechnya who were dormant for years are now fighting in Syria. When they return home, people idolize them. They then become useful tools for recruitment and radicalization.

Additionally, al Qaeda utilizes the Internet and technology to expand their efforts and reach a broader "audience" with minimal efforts and resources. Leaders can have an impact and a foothold in a country without ever stepping foot inside its borders, including through online recruitment and training. The recent conflict in Syria has increased radicalization efforts because it attracts young individuals to the fight abroad through the use of social media, especially from the United Kingdom and Canada.

> ***"Looking ahead is never easy. The best way to predict the future is to shape it."***

It is extremely convenient to travel between Syria and the United Kingdom. It is difficult for law enforcement to determine a person's reason for travel because there is a large humanitarian effort in the region in addition to the fighting. Even if a person travels to fight, it is hard to know which side they support. The real concern is when radicalized individuals return home with training because it is hard to determine at what point an individual might decide to engage in extremist violence at home. Also, the panel noted that the radicalized individuals tend to be educated with resources, which makes prediction more difficult.

The Internet created a new threat – cyber attacks – which is significant and provides means for actors to attack a country without physically stepping foot in it. Iran and North Korea pose the biggest threat to cyber security. There have already been numerous attacks resulting in stolen intellectual property and identities costing individuals, corporations, and governments billions of dollars. These countries do not have the capacity to develop technology to wage cyber attacks so they buy it from countries like Russia and China.

Technology and the Internet have clearly escalated the complexity of the threat and expertise required to mitigate and investigate these crimes. Investigations have become transnational, which brings along new challenges – legal boundaries, human rights considerations, and limitations on evidence gathering. Law enforcement needs to adapt and respond through effective intelligence gathering and prosecutions encompassing all stakeholders in a unified response – local, national, and international. Additionally, legislative improvements are needed in all countries to foster more effective information sharing.

There has been no national debate regarding how to access, manipulate, and harvest digital information like there has been related to information collection in the physical world. This is evident by the lack of laws pertaining to or, at times, restricting law enforcement's use of the

Internet to investigate and monitor subjects. Just because everyone leaves a digital footprint that makes locating and tracking easier, it does not mean law enforcement should have unfettered access to the information without obtaining appropriate court orders. Therefore, the debate needs to happen and appropriate laws need to be enacted to ensure civil right and civil liberties are protected.

The public perceives law enforcement as security professionals who should know where a person is because of their digital footprint, not simply as reactive law enforcement professionals. Therefore, law enforcement needs to redefine its responsibilities to match public perception. This entails redefining what a "case" is. It can no longer be defined by what can be prosecuted, but rather by identifying and understanding the network through exploiting digital information. To be preventative, we need to work together. For instance in the United States, fusion centers can be used to draw a picture of a network and design take downs destined to gut an organization rather than arrest an individual. In the age of globalization, no case can be defined by a jurisdiction; therefore, investigation should be international collaborations.

Fusion centers are problematic in how they are implemented as well as how they are understood across the United States. They are too narrowly focused and need to expand to an all-crimes approach. In this age of globalization, crime crosses jurisdictions and the adversary is a network, not an individual. Today, drugs, gang violence, and child pornography are bigger threats to the United States than terrorism ever was or will be. However, local law enforcement does not have the software tools to deal with global networks, so the fusion center is the answer. They have the analytical power, but currently they do not have the training, the relationships and expectations with local jurisdictions, or the software to do so. In 2020, we cannot still be questioning the value of fusion centers.

An overall theme through the panel was that homeland security is a shared responsibility with the communities they serve. Therefore, community engagement is vital. Law enforcement needs to deliver a message that everyone has a stake in this fight and a meaningful response to homeland security has to be done in partnership with the communities. We need to engage the community, listen to their needs, and understand their concerns. Programs have to be delivered by the community to the community.

Looking ahead is never easy. The best way for law enforcement to predict the future is to shape it. Today, society and technology are creating an environment more difficult for an adversary. In a democracy, countries can never be 100% secure, but they need to identify the highest risks and protect the most vulnerable and likely targets.

Day 1, Panel 3 – Threat Evolution: The Virtual (Cyber Warfare)

- Moderator – **Mike Haley**, Sheriff, Washoe County, Reno, Nevada
- **Justin Vallese**, Supervisory Specialist, Federal Bureau of Investigation
- **John Amrine**, Colonel, Senior Advisor, Space and Missile Systems Center
- **Dr. Blaine Burnham**, Strategic Initiatives, Information Sciences Institute, University of Southern California

Collaboration: The Virtual (Cyber Warfare)

Building Partnerships: Working together and sharing information is the only way to combat a global threat.

Embracing Social Media: Even the playing field with terrorist organizations and transition into the digital age.

Enhancing Cyber Capabilities: Train and educate all levels of employees that have access to systems vulnerable to attack.

Ensuring Global Information Exchange: Amend legislation to allow for international investigations.

This panel focused on the threat in the United States, but as widely discussed throughout the conference, globalization of criminal activity makes this relevant to all the Five Eyes. From the FBI's perspective, cyber attacks are a top threat. Perpetrators range from nation state actors to sophisticated organized crime organizations to hackers for hire. They steal intelligence and national security data as well as trade secrets and valuable research from companies, universities, and governmental entities. For example, one company lost 10 years of research and development work to a foreign adversary overnight worth one billion dollars. These attacks are initiated overseas, so it requires a great deal of training and expertise to investigate these crimes. Also, due to the nature of the crime, not all attacks are reported or even detected, making it difficult to grasp the full scope of the cyber threat.

There are different types of actors engaging in cyber crimes than traditional crime. For instance, a 15-year-old in Canada shut shutdown eBay, Yahoo, E*Trade, Global Crossing, and CNN just to see if he could do it. On the flip side, known terrorist organizations steal personal information and financial data to fund operations. The FBI classifies cyber attacks in five ways,

keeping in mind some can overlap: hacktivism, cyber crime, industrial espionage, cyber terrorism, and state-sponsored cyber disruptions.

Hacktivism essentially involves "activists who hack," like with the Anonymous group. There is no financial motivation in their activities. Their objective is to exploit computers and technology to further their cause. The FBI also categorizes hacktivism as cyber crime, which is defined below. This threat will change moving forward. As systems become more secure, successful attacks will decrease. As a result, the hactivists' misinformation campaigns will increase in an attempt to keep the message alive and relevant in the media.

Cyber crime is financially motivated and exploits software and hardware vulnerabilities to access information to sell to the highest bidder. Cyber criminals mostly operate through online forums. For example, three Eastern Europeans were charged with spreading the "Gozi" computer virus to more than one million computers at financial institutions using a PDF file, producing more than $50 million in illegal profits. These criminals never had to set foot in any of their international targets thanks to the Internet. These international attacks require international investigations and cooperation to mitigate.

Industrial espionage comes in two forms. The first is economic espionage, which involves the collection of sensitive U.S. economic information and technologies and is conducted heavily by China and Russia. State espionage involves foreign actors aggressively targeting corporations to steal intellectual property for financial or strategic gain not as an act of terrorism or war. The estimated loss for the United States to date from state espionage is between $2 billion and $400 billion. It is difficult to put a value on the stolen information because it is often difficult to identify what has been stolen. Industrial espionage conducted by nation states can be loud and easily detected with the objective of stealing in bulk or it can be done covertly to seek quality information, such as intellectual property. When seeking precise information, the actors use a computer intrusion that imbeds malware or code that allows a real time, continuous presence on a computer, also known as an Advanced Persistent Threat. These types of attacks have been extremely successful at obtaining proprietary information, such as source code, negotiation tactics, and strategic operation plans.

Cyber terrorism can be conducted for financial gain or as an act of war. Cyber terrorism that uses the internet to grow the "business" of a terrorist organization and connect with like-minded individuals focuses on raising money and recruitment. They can attack remotely without ever stepping foot in the targeted country. There have not been many successful attacks; therefore, this is an emerging threat. In the future, cyber terrorism may target critical infrastructure, incident command systems, air traffic control systems, or navigation systems critical to aircraft; therefore, investing in protection today is imperative for a safe tomorrow.

State-sponsored cyber disruptions as an act of war is an evolving category, but the United States is currently focusing on how to neutralize attacks and defend military networks. At this time, because certain actions overlap categories, it is difficult to define state-sponsored cyber

disruptions as an act of war. However, computer network warfare is evolving so rapidly there is a mismatch between our technical capability to conduct operations and the governing laws and policies for those operations.

As we move forward, planning ahead and investing are important. Laws need amending to allow international investigations and make them easier. This will not succeed, however, if relationships of trust are not in place first. The only way to combat a global threat is by working together and sharing information.

The largest attack on a state government organization to date took place recently in South Carolina. The attack occurred on August 13, 2012, when the initial phishing email sent from Russia was opened by an employee at the South Carolina Department of Revenue. The email contained a tool that gathered department emails and passwords. This then allowed the criminal actor to access the secure servers and mine personal identifying information of 75% of South Carolina's citizens (e.g., dates of birth, social security numbers, bank accounts, and credit card numbers). The investigation and apprehension of the criminals occurred relatively quickly in October of 2012, but it was too late. Had the recommended $20,000 software been installed and the employees trained properly, $40 million dollars in damage would not have occurred. When information like this is stolen, criminals and terrorists not only fund their operations, they can also create new identities that allow them to travel freely, without detection.

The takeaways from this real-life example are:

- Terrorists have already transitioned into the digital age, so security professional must.
- Training all employees who have access to a computer is just as imperative as having the proper software in place.
- Leadership must be onboard and invest in the emerging threats.

The following resources were provided for further education on the cyber threat:

- U.S. Presidential Executive Order – Improving Critical Infrastructure Cybersecurity[1]
- Digital Appendix and Indicators, Mandiant[2]
- APT1: Exposing One of China's Cyber Espionage Units, Mandiant[3]
- Director National Intelligence, James R. Clapper Statement for the Record, U.S. Senate Select Committee on Intelligence[4]

[1] http://www.intelligence.senate.gov/130312/clapper.pdf
[2] http://intelreport.mandiant.com/
[3] http://intelreport.mandiant.com/
[4] http://www.intelligence.senate.gov/130312/clapper.pdf

Day 2, Panel 1 – Operational Approaches

- Moderator – **Peter Dein**, Assistant Commissioner, New South Wales Police Force
- **Doug Best**, Superintendent, Royal Canadian Mounted Police
- **John Parkinson**, Retired Chief Constable, West Yorkshire Police
- **Larry Brooks**, Director General, Canadian Security Intelligence Service
- **Neil Gaughan**, Assistant Commissioner, Australian Federal Police

Collaboration: Operational Approaches

Building Partnerships: Collocation of intelligence and law enforcement is imperative to foster information sharing and institutionalize relationships within an organization rather than relying on personally developed relationships.

Countering Violence Extremism: Share information with the community and engage community leaders to develop counter narrative messaging strategies.

Ensuring Global Information Exchange: Share information globally as the threat is ever changing and evolving.

This panel discussed the progression of homeland security operations across Australia, Canada, and the United Kingdom. The panelists discussed a variety of topics: the evolution of counter-terrorism efforts, the importance of solidifying relationships within an organization rather than through personal relationships, the benefits of engaging the community, and legal obstacles faced when turning intelligence into evidence. These topics all dealt with improving information sharing efforts and aligning operations to match public expectation that all branches of law enforcement and intelligence work together seamlessly. As public scrutiny has increased and the realization this is not happening, it has forced barriers to be broken.

For instance, in the United Kingdom, the police force and intelligence forces are completely separate entities. Originally, there was not a widespread desire to work together, and it was only done when one entity needed the other. However, around 2005, the intelligence forces began transitioning to regional stations rather than the one, centrally located entity in London. This regionalization coincided with changes with the police force to bring together its covert functions with its investigative capabilities. The London bombings accelerated the pace of change and highlighted the public's lack of understanding as to why different forces cannot share everything. This intense scrutiny led to collaboration and collocation of assets to

physically work alongside one another. Joint tasking, operations, and briefings have become the norm. Additionally, informants are now mapped by geography, environment, and affiliation to create a clearer picture for gap analysis and targeted activity. This change created a genuine fusion of skill sets, not just collocation of resources.

Relationships need to be institutionalized internationally, nationally, and locally among law enforcement and intelligence agencies. For Australia, terrorist attacks in foreign countries result in the overwhelming amount of deaths to their citizens. Therefore, the Australian Federal Police requires strong deployment plans to rapidly respond to incidents and provide forensic support and victim identification in foreign nations. The struggle remains on how to institutionalize partnerships within an organization rather than rely on personal relationships.

Laws and case law can also help to institutionalize relationships. In Canada, the judicial and intelligence branches decided to establish a framework for the two organizations to successfully collaborate, work together, and break down the barriers hindering the transitioning of intelligence to evidence. Striking this balance is extremely difficult, so they established a working group to identify best practices from around the world by monitoring recent incidents and case law to assess how intelligence was turned into evidence. The ultimate goal was to develop guidelines applicable to both organizations to alleviate the tension between the judicial and intelligence process. They assessed each organization and focused on core principles. Additionally, each guideline was supported by case law and linked to the relevant decisions so practitioners could better understand the guidelines. The main concern identified was managing disclosure obligations and how each organization would share information while staying in compliance with legal restrictions. Therefore, it was imperative to develop a strategy to transition this information from one to another.

The Canadian Police also discussed the importance of engaging the community to build relationships. Oftentimes, the community comes to law enforcement with vital information. Therefore, prior to the release of information, it can be useful to meet with community leaders so law enforcement and the community can have one, consistent message. Additionally, law enforcement should utilize the community to get ahead of the al Qaeda narrative by creating counter messaging efforts with community leaders for them to deliver to their own.

Even though each panelist approached this topic differently, they all emphasized the importance of relationships from the local community to the international level. Sharing information and collaborating is imperative with the ever changing threat environment.

Day 3, Panel 1 – Meeting the Needs of the Victims of Terrorism from Prevention

- Moderator – **Sue O'Sullivan**, Retired Deputy Chief, Ottawa Police Service, Federal Ombudsman for Victims of Crime, Canada
- **Susheel Gupta**, Chairman and CEO, Air India Victims' Families Association
- **Kristin Aga**, Superintendent, Oslo Police District, Norway
- **Mary Fetchet**, Founding Director of Voices of September 11th

Collaboration: Meeting the Needs of the Victims of Terrorism from Prevention

Building Partnerships: Engage victim assistance organizations to understand from a victim's perspective how to improve response.

Conducting Exercises and Training: Include victim assistance organizations in exercises and training to ensure smooth operations at the time of an incident.

To begin the discussion, the panel highlighted and praised a few initiatives of conference attendee Maureen Basnicki, a Canadian citizen widowed as a result of the September 11th attacks. She is the co-founder of Canadian Coalition Against Terror[5], which led the campaign for the passage of Justice for Victims of Terrorism Act of 2012[6] that enables plaintiffs to bring lawsuits against terrorists and supporters of terrorism. September 11th was declared a National Day of Service thanks to Ms. Basnicki's efforts. She also spearheaded the creation of the Alliance of Victims of Terror, a charity which provides "education, support, and public awareness…on the effect of terrorist violence on the individual, the community and society. They provide assistance to those whose lives have been impacted by terrorist violence and promote civic participation through volunteerism, to encourage and strengthen individual and community-based resilience."[7] The panel went on to discuss how victims can assist in a more

> ***"The faces to remember in terrorism are the victims."***

effective response. An integral part of the LinCT AA is and always has been to have the voice of victims at the conference. The panel highlighted incidents in three countries that should shape the way forward. Combatting terrorism is as much about stopping the action as it is about supporting the victims. This panel allowed law enforcement the opportunity to view

[5] http://www.c-catcanada.org/
[6] http://laws-lois.justice.gc.ca/eng/acts/J-2.5/page-1.html
[7] http://www.actvfoundation.org/

their efforts through the eyes of the victims to better understand how it affects them and areas that need to be changed moving forward. That is not to say there have not been great strides in this area. As the discussion showed, victims are much more a part of the process today than they used to be, but there is always a need for improvement.

For instance, after the Air India bombing, victim assistance did not exist and the government did not reach out to victims for more than ten years after the incident only when the RCMP decided to break with protocol and contact the victims' families to update them on the investigation. Major changes did not occur in Canada until September 11th. Only then, was a full investigation launched into the Air India bombing. The 20-year delay was because people were afraid to place blame. In fact, a few years after the bombing many victims' families were urged to sign agreements to not sue so emphasis would be on improve and not placing blame. Today, efforts are underway to improve victim assistance.

Learning from failures, police departments are now assigning a Family Liaison Officer (FLO) to families affected by terrorist incidents. This provides the family with a direct line of communication with the investigators. During the 2011 Norway attacks, the benefit of the FLO was realized and is now part of the national law enforcement effort. All officers going through the academy now take a class on family liaison work, and all districts within the country have FLOs and coordinators. It is imperative to employ and train officers who specialize in victim assistance. This allows for information to flow naturally and quickly. Ideal tasks and things to consider are as follows:

- Assign each victim's family at least one FLO.
- Maintain constant contact with the victim and/or their family to avoid frustration from lack of information/misinformation.
- Identify one family member as the main point of contact, if possible, so the family knows unless the FLO has spoken directly with the main contact, the information may not be accurate.
- Establish scheduled times to provide updates to the family. This is extremely important for victim identification to avoid families being nervous or anxious about getting bad news every time the phone rings.
- In the event there are problems within families (e.g., there are family members that do not communicate with one another) it may be necessary to assign multiple officers and/or identify multiple points of contact within a family so all members are informed.
- Utilize national criminal investigative services for identifying victims.
- Keep families informed at all times and give them information before a press conference.
- Make a detailed report about how each victim was injured/died because the family usually wants to know. In the event a victim died in the presence of someone else, it can be comforting to family to know they were not alone.
- Maintain constant contact with the head of the investigation to obtain the most accurate and up-to-date information.
- Prepare the family for any media events or how to handle the media attention.

After a terrorist event, returning to regular life activities can be difficult for victims and their families. Most often, they are in need of mental and physical health care. Advocacy groups and charitable organization can help with victim assistance after an incident with both monetary and psychological support. For instance, when the mass shooting occurred in the United States at Virginia Polytechnic Institute and State University at the end of the school year in 2007, victims had to leave school and return to their parents' home for the summer. This created a logistical issue for how to ensure the students received proper victim assistance after the shooting, so the staff connected them with services near their homes. Advocacy groups can be integral in ensuring victims and families receive what they needed.

Additionally, the advocacy group work sometimes is just beginning once a crisis ends, highlighting the importance of the need for a transition plan from FLOs to support/community groups. Therefore, victim assistance needs to be part of pre-incident event efforts and involved in planning and exercising. This will establish relationships beforehand and allow for a smooth transition to life after an incident. The Voices of September 11th[8] organization recognized this difficulty and the complications the families and victims have navigating the assistance process. They conducted a study of incidents over the years and gathered the best practices for helping families and victims. The organization is developing a "tool kit" for integrating victim services into the law enforcement efforts. It will be available online upon completion.

[8] http://www.voicesofseptember11.org/dev/index.php

Day 3, Panel 2 – The Role of Private Industry: Protecting High Value Targets

- Moderator – **Brian MacDonald**, Inspector, Transit British Columbia
- **Brian Brady**, Vice President and Deputy Chief Security Manager, NBC Universal Studios
- **Michael Julian**, General Manager Security, Westfield Corporation, Australia
- **Arif Alikhan**, Director of Airport Police & Deputy Executive Director for Homeland Security, Fire/EMS, and Law Enforcement, Los Angeles World Airports

Collaboration: Protecting High Value Targets

Building Partnerships: Build partnerships between the public and private sector and come together to solve identified problems that result in structural changes.

Conducting Exercises and Training: Include private sector in training and exercises to better prepare for an incident.

Performing Risk-Based Security Exchange: Discuss risk-based security principles with senior executives because this is language they are familiar with and employ risk-based security to minimize disruptions affecting the bottom line.

The panelists consisted of former law enforcement working in the transportation, entertainment, and retail industries. Collectively, they discussed the risks and challenges faced by both the private and public sectors as well as how each can work together and help each other mitigate the risks and challenges.

In the public sector, the primary mission is safety and security while in the private sector the primary mission is to operate a business which results in safety and security as support functions. The priority in the private sector is about customers and cost, which means making sure customers have the most enjoyable experience in the most cost effective way. Therefore, working with corporate senior executives can be a challenge because their priorities and functions are to run a business.

Senior corporate executives are not familiar with law enforcement language, priorities, and threats resulting in a lack of understanding and a struggle to incorporate security needs into the business model. Furthermore, they are used to seeing metrics for success to justify the spending. In law enforcement, success is measured by the absence of an incident and does not correlate to graphs and statistics. Therefore, proving a return on investment can be difficult in

the private sector. As a result, it becomes imperative to humanize the issues rather than just talking policy in the abstract and to educate senior executives on the threats and challenges faced by law enforcement. It is helpful to remind senior executives that they are protecting people, not things. They are protecting children, aunts, uncles, and parents.

To demonstrate a return on investment, it is always helpful to switch dialog to business terms. For instance, speak about risk management (a concept used heavily in the financial world). Security is a cost function that does not generate income. It only uses money. Therefore, discussing how security can reduce the risk of an incident that can result in a public relations nightmare will be seen as favorable. However, manage expectations. As Gordon Graham discussed earlier in the conference, it is the principle of "what's knowable is preventable;" however, this is not to suggest that everything is preventable. But, injury and death can be mitigated by investing in training and exercising. This helps establish relationships before they are needed.

The private sector, like the public sector, will benefit from investing in building relationships with the law enforcement and other first responders. Partnerships are a mutual obligation. Both sectors need to come together to solve identified problems and make structural changes within each organization to enhance partnerships. For instance, Universal Studios has law enforcement days where they bring in first responders, allow them to tour the facilities, and provide them with map books specifically designed for use during incident responses. This way, first responders will be prepared and familiar with the facilities coming into an incident as opposed to having to learn on the fly.

"See Something, Say Something USEFUL."

One panelist suggested there needs to be a shift in the way private sector assets are protected. Security professionals need to stop using phrases such as "better safe than sorry" or "See Something, Say Something." He suggests these have done more harm than good to the private sector. For instance, every time there is an unattended package, a shopping mall cannot be shut down or there will be millions in lost profits.

The suggested alternative method is "HOT ALERTS: Guidelines for Assessing Whether Found Property Is Suspicious."[9] Security should "Get the F.A.C.T.S."

[9] http://www.secure.nsw.gov.au/Business-network/

- ✓ Find the Owner: interview people and use video surveillance
- ✓ Assess the Property: use HOTALERTS guidelines
  - H – Is it Hidden?
  - O – Is it Obvious?
  - T – Is it Typical?
  - ALE – Is the government Alert Level Elevated?
  - RT – Is the location in Receipt of a Threat?
  - S – Is the property found in a Sensitive location?
- ✓ Consider The Situation: view the conduct of the owner, environmental factors, and other suspicious factors as a whole

The principle of HOT ALERTS can be useful if the abandoned package is a shoe box from a retailer in the shopping center. A person most likely bought new shoes, put them on, and left their old ones behind. In the private sector, it is important to not waste resources and interrupt business unnecessarily. So, if there is no credible threat about an attack on the establishment, the chances there is a bomb is very minimal. Do not be afraid of approaching the person or a suspected terrorist. Ask basic questions to get as much information as possible.

Breakout Sessions

Home Grown Violent Extremism and Countering the Local Threat

- Moderator – **Mike Ferrence**, Associate Director, Major County Sheriffs' Association; Executive Director, Leadership in Counter Terrorism Alumni Association
- **Irfan Saeed**, Senior Policy Advisor, U.S. Department of Homeland Security, Office of the Secretary and Office for Civil Rights and Civil Liberties

Collaboration: Home Grown Violent Extremism and Countering the Local Threat

Building Partnerships: Engage the community to develop counter messaging and respond to the threat with the strength of the community.

Countering Violence Extremism: Evolve with the threat to counteract violent extremism.

Embracing Social Media: Embrace social media and be creative with counter messaging as al Qaeda and others already have.

The first step in devising ways to counter violent extremism is to define the issue. According to Erroll Southers, Associate Director of Research Transition at University of Southern California's CREATE center, homegrown violent extremists are U.S. citizens or residents who embrace a violent ideology largely within the United States. They can operate either domestically or overseas. Violent extremists typically display three precursors as they travel down the road to acting on their violent beliefs: 1) they are open to extremist views; 2) they relate to a stated grievance; and 3) they seek out a community of interest.

There is not one type of homegrown violent extremist. Rather, there has been an evolution of the terrorist threat over the past several decades. From 1990 to 2001, the threat was largely overseas and the focus was on large-scale attacks. Law enforcement adapted and laws were passed to allow for better information sharing and international collaboration to harden borders. After 2001, al Qaeda adapted to the changes and focused on collecting finances. Laws and law enforcement adapted, so al Qaeda adapted again and decided to radicalize from within. Around 2005, social media exploded. It allowed for al Qaeda to create videos and propaganda to spread internationally by exploiting the media and the Internet to distribute its narrative. Additionally, scandals like Abu Ghraib and a range of U.S. policy changes occurred, providing fodder for recruitment. Al Qaeda understands how to use these types of events to

create propaganda whereas law enforcement and policy makers do not. Even though Western policies are not the cause of violent extremism, al Qaeda has turned them into drivers of violent extremism. They managed to craft jihadi messaging as "cool" and developed English language outlets to increase their reach (e.g., *Inspire* magazine).

Between September 2007 and October 2009, only about 20 men left the Minneapolis area to fight for al-Shabaab, an al Qaeda affiliate in Somalia. Those numbers pale in comparison to the numbers today. To counter the narrative that is creating this exodus to fight for al Qaeda, law enforcement needs to go into the communities and tell them, "We aren't targeting you. We are trying to bring attention [to the problem]." Law enforcement should respond to the threat with the strength of communities. Local partners become "drivers" of the effort to counter violent extremism, so sharing threat information with community members is imperative.

For example, two communities in the United States have created videos and advertisements to counter the al Qaeda narrative. In Minneapolis, Minnesota, the community created a video called "Truth about al Shabaab." It tells viewers they will die. They will be used as a suicide bomber or killed if they refuse. Also, a group in Chicago is on a mission to take back the phrase "My jihad is to …" from terrorists and use it positively, which might include "My jihad is to work in a soup kitchen."

Bottom line, law enforcement does not have a counter narrative but they can give communities information so to develop their own counter narrative. Efforts need to shift to a proactive approach rather than reactive.

Using Social Media for Development of Leads and the Impact on Counter-Terrorism Efforts

- Moderator – **Dr. David Corderman, Associate Executive Director LinCT Alumni Association**
- **Jim Chu**, Chief Constable, Vancouver Police Department

Collaboration: Using Social Media for Development of Leads and the Impact on Counter-terrorism Efforts

Building Partnerships: Engage the community in a language they understand and utilize in real time.

Embracing Social Media: Utilize the information placed on the Internet to enhance and support investigations.

Enhancing Cyber Capabilities: Enhance capabilities to ensure social media can be used and is reliable.

Social media is extremely helpful for law enforcement. Knowing this and seeing firsthand the benefits, Vancouver Police Department employs two full-time media liaison officers. Also, Chief Constable Chu hosts his own online "talk show" on YouTube and holds "Tweet the Chief" events to answer questions from the public. This personalizes law enforcement, especially for the youth audience, and speaks to them in a media they use and are familiar with.

Social media is the way of the future, so law enforcement needs to use it. It allows for daily communication with the public and can be used to:

- Provide real-time information to the public areas of concern
- Repair or recoup public image in the event of police misconduct
- Increase public confidence in law enforcement by informing them the situation is under control or being taken care of
- Locate and track vigilantes to control riots
- Produce evidence
- Identify and locate criminals
- Control messaging to the public to potentially prevent misinformation by media outlets

Law enforcement can be its own media source. It is best to get ahead of a story and give the public information firsthand. Also, law enforcement should rely on the public to police itself. During the riots following the 2011 Stanley Cup, people created websites outing people who committed crimes and sent photos into the police department. Law enforcement created bulletins of the photos received and released it to the public through media outlets and handouts on college campuses to assist with identifying criminals. Also, Vancouver Police Department's Integrated Riot Investigation Team created a website for identifying rioters - https://riot2011.vpd.ca/.

Top Surprises when Dealing with Social Media

1. People will tell you where they are and where they are going. They will post pictures of themselves committing crimes, but law enforcement must capture the information the moment it is seen. Information can be taken down as quickly as it is put up.
2. In the era of smartphones, there is most likely someone who captures something of value. Also, there is a great deal of information to sift through (e.g., posts, videos, pictures). This can result in a delay in filing charges because of the number of hours and personnel required to sift through all the information. The public expects accountability quickly, but the urge must be resisted so all people responsible can be punished for every crime they commit. Just because a person is seen in one photo doing something, doesn't mean there are not more photos of them committing other crimes. During the riots following the 2011 Stanley Cup, the Vancouver Police Department did not file any charges for five months despite public scrutiny to do so. They reviewed all the footage and catalogued it first. There is a risk of hacking, but law enforcement social media operators must be vigilant about checking their systems and preventing attacks. However, that is a risk worth taking because of the value of the information received and produced.

> ***"It's better to be right, not quick."***
>
> - Jim Chu, Chief Constable

Honorary Associates Induction

For the first time, the LinCT Alumni Association inducted two people as Honorary Associates for their work in furthering victim assistance – Mary and Frank Fetchet. They lost their son on September 11th and established Voices of September 11th.[10] The organization provides a range of services for rescue workers, survivors, and families of the fallen. They assist with case management, special events, education, support groups, and so much more. Mary and Frank are part of the LinCT AA family, and we are happy to have them.

[10] http://www.voicesofseptember11.org/dev/index.php

Speakers

Kristin Aga
Superintendent
Violent Crime Unit of Oslo Police District

Kristin Aga graduated from the Norwegian Police University College in 1998 and studied criminology and psychology at university level. During her police career she has focused on family liaison work. Before she started her police career she worked with children and adults in psychiatric care.

In 2004 she was employed by the Violent Crime Unit of Oslo Police District where she is still working as a Police Superintendent specializing in family liaison work. The main task of the Violent Crime Unit is to investigate homicide and attempted homicide. She has always been dedicated to dealing with family members. In 2004 she was the family liaison officer for several families involved in the tsunami, and had an important role related to the identification of Norwegian victims.

During the terrorist attacks in Norway on 22 July 2011 she was responsible contacting the families of the 77 deceased. She managed a group of 30 family liaison officers from the 27 police districts involved.

She is a member of the national identification group of KRIPOS (The National Criminal Investigation Service) and a member of a group working to develop a new course at the National Police University College for family liaison issues. Based on experience from the tsunami and the terrorist attacks on the Government buildings and Utøya in July 2011, she liaison issues. Based on experience from the tsunami and the terrorist attacks on the Government buildings and Utøya in July 2011, she has obtained substantial experience within family liaison work.

Arik Alikhan
Director of Airport Police & Deputy Executive Director for Homeland Security, Fire/EMS, and Law Enforcement Los Angeles World Airports (LAX, ONT, VNY)

Arif Alikhan recently joined Los Angeles World Airports as its new Director of Airport Police and Deputy Executive Director for Homeland Security and Law Enforcement. Director Alikhan is responsible for overseeing the 1,100 civilian and sworn law enforcement personnel of the Los Angeles World Airports Police Department and over 100 firefighter and paramedics responsible for protecting Los Angeles International, Ontario International, and Van Nuys Airports.

Prior to his appointment, Director Alikhan served as a Distinguished Professor of Homeland Security and Counterterrorism at National Defense University's College of International Security Affairs in Washington.

In 2009 Director Alikhan was appointed to the Obama Administration as the Assistant Secretary for Policy Development at the U.S. Department of Homeland Security. Prior to his appointment to the Administration, Director Alikhan was the Deputy Mayor for Homeland Security and Public Safety for the City of Los Angeles.

His legal experience includes serving as a federal prosecutor in Los Angeles, as the first chief of the Cyber and Intellectual Property Crimes Section for the U.S. Attorney's Office, and as a senior advisor to two U.S. Attorneys General on civil and criminal intellectual property initiatives and cybercrime issues.

Chris Allison
Assistant Commissioner
Metropolitan Police Service

Chris Allison has been in the Metropolitan Police Service (MPS) for the whole of his policing career and for the majority of those 29 years, this has been as a uniformed officer. He is currently the National Olympic Security Coordinator and was responsible for coordinating the planning and delivery of the security operation for the Olympics and Paralympics in 2012.

Throughout his service, he has been heavily involved in the policing of public order events, these ranging from ceremonial events, football matches, small marches and demonstrations, all the way through to the resolution of severe public disorder.

Since 1996, he has been a member of the MPS Advanced Public Order Command Cadre and he is also a member of all of the other Command Cadres in the Met. As a part of these Cadres, he has undertaken a command or oversight role at most of the major events and incidents in London over the last few years. He was the Police Gold Commander for the terrorist atrocities that took place on the London Underground on the 7th July 2005 for which he was awarded an MBE.

In the past, he has undertaken the Association of Chief Police Officers (ACPO) lead on licensing / alcohol matters and the ACPO lead for Chemical, Biological, Radiological and Nuclear (CBRN) matters. He is now the head of the ACPO Olympic Business Area.

John M. Amrine

John Amrine serves in a senior executive role as an IPA to the Commander of the Space and Missile Systems Center (SMC) located at Los Angeles Air Force Base. As a Senior Technical Advisor, he forges new strategic partnerships between the SMC programs and the Intelligence Community. The goal of these partnerships is to optimize space systems through collaboration. In addition, he provides outreach to the war fighter to ensure they are aware of new effects from space as well as proposing and testing innovative uses of space systems to meet war fighting requirements. He also serves as the deputy of the NSA/F81 Field Office that is collocated with SMC and is responsible for providing Information Assurance support to all SMC programs.

Additionally, Mr. Amrine is responsible for regularly taking Air Force Space Command general officers and civilian seniors back to US CYBER Command and the National Security Agency for executive immersions into the cyber domain. He further assists Air Force Space Command protect their OPS centers from cyber threats/vulnerabilities.

Commissioned from the Air Force Academy in 1982, Mr. Amrine held a number of assignments in space operations, acquisition, staff, and in-theater support to combat operations including assignments at the National Reconnaissance Office, National Security Agency and U.S. Space Command. He commanded at three levels: the 5th Space Surveillance Squadron at RAF Feltwell, the Space Operations Group at the Aerospace Data Facility-Colorado and the Space Based Infrared Systems Wing at Los Angeles AFB. He retired in the rank of Colonel.

Doug Best
Superintendent, Assistant Criminal Operations Officer National Security
Royal Canadian Mounted Police

A graduate of Memorial University of Newfoundland, he holds two undergraduate degrees and a graduate degree in Administration.

He began his career with the Royal Canadian Mounted Police in 1977 as a plain clothes investigator in the Toronto, Ontario area. Here, he worked in the fields of General Investigations, Organized Crime, Drug Enforcement and Commercial Crime. He joined the RCMP Security Service in 1981 and was transferred to National Headquarters where he worked on the China Desk. Doug remained with the Security Service when it became the Canadian Security Intelligence Service (CSIS). He worked in both the Counter Intelligence and Counter Terrorism fields as an Intelligence Officer. Prior to returning to the RCMP in 1996, he worked as a liaison officer with the Service's two oversight bodies, the Security Intelligence Review Committee (SIRC) and the Inspector General's Office (IG).

Following his return to the RCMP, Doug was assigned to the Air India bombing Investigation, Vancouver, British Columbia, where he held the role of Lead Investigator and Operations Officer. He was commissioned in 2006 and took on a variety of senior roles in National Security, Protective Operations and Border Integrity in British Columbia before taking his current role in Ontario.

Over his career, he is particularly proud of his collaborative work with national and international partner agencies.

John Boutcher
Assistant Chief Constable
Joint Protective Services

Jon holds the post of Assistant Chief Constable Joint Protective Services which includes major crime, scientific services, roads policing, dogs, armed policing and public order and civil contingencies.

He is the ACPO lead for Crime under the Children and Young Persons group and the ACPO lead on legislation relating to covert policing (RIPA) within the Crime Business area. As well as his national responsibilities as an ACPO CT Commander he was the Hertfordshire Gold Commander overseeing the Hertfordshire venue for the London 2012 Olympics.

Jon has 27 years' service spent mainly as a Detective in covert and proactive policing roles. He has also worked on Regional and National Crime Squads, targeting serious and organized crime groups with links to international networks and was responsible for a section of the 'Flying Squad' in London.

In 2003 Jon joined the Anti-Terrorist Branch at New Scotland Yard as the Senior Officer for numerous national security operations. Jon was responsible for the 'manhunt' that identified and arrested the 21/7 failed terrorist plotters. He also led the investigation in Scotland following the Glasgow airport terrorist attack.

He has worked within the Home Office as an advisor on Policing issues specifically related to national security and counter terrorism.

Brian Brady
Vice President and Deputy Chief Security Officer, Security and Crisis Management NBC Universal

Currently Mr. Brady is the Vice President and Deputy Chief Security Officer, Security and Crisis Management, NBC Universal and joined NBC Universal in January of 2005. He served more than 34 years in Municipal Law Enforcement, with the cities of Berkeley, Baldwin Park and Novato, California; and in Farmington, New Mexico.

He has worked virtually all police assignments, including Patrol, Investigations, Traffic, Administrative, and Specialty Assignments i.e. SWAT and Crisis Management. He retired in December of 2003 as the Police Chief with the City of Novato, in the San Francisco Bay Area.

He owned and managed a Training and Consulting Company providing specialized training for Federal, State, County and Municipal Law Enforcement personnel. Under contract to the US Government, provided specialized training to military personnel. He has provided protective services and management for major events and for celebrity clients. Brian Brady has a BA from Golden Gate University, San Francisco; MS, Madison University and California State University, Sonoma.

Larry Brooks
Director General Middle East & Africa
Canada Security Intelligence Service

Larry Brooks is the Director General of Middle East and Africa operations CSIS. A graduate of Queens University, he began his career in 1976 with the Royal Canadian Mounted Police (RCMP) as a uniformed officer. Joining the newly formed CSIS in 1985 in Toronto, he was transferred to HQ in 1990 working primarily in Counter-Terrorism (CT) operations and as Parliamentary liaison from 1998 -2000. Returning to Toronto in 2002, he managed CT operations for Southern Ontario and in 2007 was posted to London, UK, as Head of Station.

Working closely with RCMP counterparts, Mr. Brooks was the CSIS line manager responsible for the investigation and prosecution of the "Toronto 18" case. This major CT operation resulted in the successful prosecution of the conspirators and their associates in Canada, the USA and Europe. In recognition of this highly successful operation, both agencies were awarded the Booz Allen Hamilton Outstanding Achievement in the International Prevention of Terrorism Award in May 2011.

Recently, Mr. Brooks co-chaired a working group tasked to develop operational guidelines for CSIS and the RCMP to ensure a practical and judicially acceptable balance between intelligence and evidence. Referred to now as the One Vision initiative, these guidelines from working standard for Canadian national security investigations.

Jim Chu
Chief Constable
Vancouver Police Department

Jim Chu, a 34-year veteran with the Vancouver Police Department (VPD), was appointed Chief Constable in August 2007. He is also the current President of the Canadian Association of Chiefs of Police.

He joined the VPD in 1979. His early assignments included patrol constable, School Liaison officer, and Planning and Research. He was promoted to corporal in 1989 and then detective in 1990. He held investigative assignments in the General Investigation and Robbery Squads, then returned to patrol as a sergeant in 1991. In 1996, he was assigned to head the Recruiting Unit.

In 1997, Jim was promoted to inspector and became the Vancouver Police Project Manager on the E-Comm project. This entailed managing the VPD transitions onto the E-Comm radio system, the new dispatch facility, the PRIME-BC Records Management system, and a new mobile computing and data access platform. He then returned to patrol as a district commander in 2001. He was promoted to Deputy Chief in 2003.

Jim holds a bachelor of business administration degree from Simon Fraser University and a master of business administration degree from the University of British Columbia. He is a graduate of the FBI National Executive Institute.

Other related experiences include: former chair of the International Association of Chiefs of Police Law Enforcement Information Management Section; former co-chair of the Canadian Association of Chiefs of Police Informatics Committee; former Board member, Major Cities Chiefs Association; part-time contract faculty member in the Douglas College Department of Criminology, where he taught introduction to policing and community policing courses; author of the book, Law Enforcement Information Technology, © CRC Press, Boca Raton, FL, 2001; author of articles in r journals, such as Police Chief Magazine, Law and Order, Blue Line, and Canadian Police Chief magazine; former President of the Vancouver Police Officers Mess; former member of Board of Governors, Justice Institute of B.C.

He was awarded a Provincial Library Trustee Association "Super Trustee" award in 1999, as well as an honourary degree from the Justice Institute of B.C. in 2010, and a Distinguished Alumni award in 2010 from Simon Fraser University. In 2011, he was named as one of 25 "Transformational Canadians" by a national media organization.

Frank J. Cilluffo
Associate Vice President; Director, Homeland Security Policy Institute; The George Washington University

An Associate Vice President at The George Washington University, Frank J. Cilluffo leads GW's homeland security efforts on policy, research, education, and training. He directs the multi-disciplinary Homeland Security Policy Institute, a nonpartisan "think and do tank" that builds bridges between theory and practice to advance homeland security through a multi and interdisciplinary approach.

The Institute's recent policy and research agenda covers a wide range of national and homeland security matters, including counterterrorism, counter-radicalization & counter-narrative efforts, cyber threats & deterrence, transportation security, CBRN terrorism, intelligence, national resilience, emergency management, and the nexus of crime and terrorism. Cilluffo chairs HSPI's Ambassadors Roundtable Series on International Collaboration to Combat Terrorism and Insurgencies, moderates the Institute's Policy & Research Forums--which spotlight cutting-edge policy solutions and innovative research--and facilitates a variety of other programmatic events. Through the Ambassadors Roundtable Series, HSPI has engaged over thirty ambassadors and cabinet level officials in an ongoing dialogue on the counterterrorism efforts of multiple nations.

Cilluffo joined GW in April 2003 from the White House where he served as Special Assistant to the President for Homeland Security. Shortly following the September 11, 2001 terrorist attacks on the United States, Cilluffo was appointed by the President to the newly created Office of Homeland Security, and served as a principal advisor to Governor Tom Ridge.

Prior to his White House appointment, Cilluffo spent eight years in senior policy positions with the Center for Strategic & International Studies (CSIS), a Washington-based think tank. At CSIS he chaired or directed numerous committees and task forces on homeland defense, counterterrorism, transnational crime, and information warfare and information assurance.

Dr. David Corderman
Associate Executive Director
LinCT AA
Senior Partner
Academy Leadership Associates

As a senior partner of the Academy Leadership Associates, LLC (ALA), a former instructor of graduate studies in human behavior and leadership at the FBI Academy in Quantico, Virginia, and an adjunct faculty member of the University of Virginia, David S. Corderman's career in leadership, training and development spans three decades. Prior to assuming his current position with ALA, in January 2007, Dave retired from the FBI following 24 years of duty, eight and half of which were spent on the FBI's Hostage Rescue Team.

He retired as Chief of the Leadership Development Institute, where he was responsible for all the FBI's external and internal leadership development programs including the National Executive Institute, the Law Enforcement Executive Development Seminar, and the international Leadership in Counterterrorism Program. During his tenure in the FBI he received numerous awards for bravery and merit.

Michael Chertoff
Co-Founder and Chairman
Chertoff Group

As Secretary of the U.S. Department of Homeland Security (DHS) from 2005 to 2009, Mr. Chertoff led the country in blocking potential terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. His greatest successes have earned few headlines – because the important news is what didn't happen.

At The Chertoff Group, Mr. Chertoff provides high-level strategic counsel to corporate and government leaders on a broad range of security issues. Before his tenure at DHS, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit and was Assistant Attorney General of the United States, Criminal Division. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism – including the investigation of the 9/11 terrorist attacks. Mr. Chertoff is a magna cum laude graduate of Harvard College (1975) and Harvard Law School (1978).

In addition to his role at The Chertoff Group, Mr. Chertoff is also senior counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

Robert Delaney
First Assistant Director General
Attorney-General's Department

Mr. Delaney commenced employment within the Australian Intelligence Community in 1987. Between 1987 and 1998 he worked in a variety of areas including Collection, Analysis and Operational Training. In 1998 he was posted to the Australian High Commission in London as a Liaison Officer. Following his return to Australia in 2001, Mr. Delaney held a number of senior operational positions.

In December 2005, Mr. Delaney was promoted to the Senior Executive Service. In July 2006, he assumed the role of Manager New South Wales, based in Sydney.

In July 2007, Mr. Delaney was promoted to First Assistant Director-General but remained in charge of the NSW Office, managing all of the organization's activity in Australia's most populous state. Mr. Delaney also manages the Operational Capabilities Division for the Organization which provides operational support across Australia.
Mr. Delaney is the only member of the Organization's Senior Leadership Group who is permanently based outside Canberra. Mr. Delaney is married with four children.

In 2008, Mr. Delaney was elected to the position of Vice President of the Leadership in Counter Terrorism Alumni Association, representing the Pacific region. He served as President of the Alumni Association in 2011.

Michael Downing
Deputy Chief
Los Angeles Police Department, Counter – Terrorism and Special Operations Bureau

Deputy Chief Michael P. Downing is the Commanding Officer, Counter-Terrorism and Special Operations Bureau where he leads five operations divisions: Major Crimes Division, Emergency Services Division, Metropolitan Division, Air Support Division, and Emergency Operations Division. These divisions include the Anti-Terrorism Intelligence Sections, Organized Crime, Surveillance Section, Hazardous Devices Section, Operations Archangel, LAX Bomb K-9 section, Special Weapons and Tactics (SWAT), Mounted Unit, Underwater Dive Team, and Emergency Preparedness and Response. Deputy Chief Downing is also a member of the Executive Board of the Los Angeles Joint Regional Intelligence Center (JRIC).

Deputy Chief Downing has testified before Congressional subcommittees relative to intelligence, homeland security and information sharing. He is a strong advocate of state and local law enforcement agencies relative to a more integrated National Intelligence Enterprise.

Michael Ferrence, Jr.,
Associate Executive Director of the Major County Sheriffs' Association
Executive Director of the Leadership in Counter Terrorism Alumni Association

Mr. Michael Ferrence, Jr., is a frequent consultant to federal, state and local law enforcement. His experience includes providing executive leadership oversight of the Major County Sheriffs' Association, the National Executive Institute, the Law Enforcement Executive Seminar, and the Leadership in Counter Terrorism Program. Each of these programs is designed to address critical issues in law enforcement at the executive level to include national and international initiatives. He is currently the Associate Executive Director of the Major County Sheriffs' Association and the Executive Director of the Leadership in Counter Terrorism Alumni Association.

Mr. Ferrence co-designed and managed the Leadership in Counter-Terrorism program, while serving as the Chief of the Leadership Development Institute at the FBI Academy, with international partners from Canada, the United Kingdom and Australia. He served in a variety of supervisory and leadership positions over his 26 year career with FBI and completed ten years of municipal police service with two years as Chief of Police. He holds a Master in Public Administration, a Master of Science Degree and is ABD PhD candidate in the field of Adult Learning and Human Resource Development.

Mary Fetchet
Founding Director
VOICES of September 11th

Mary Fetchet co-founded Voices of September 11th in 2001 following the death of her 24 year old son, Brad, at the World Trade Center. Ms. Fetchet's 19 years of experience as a clinical social has influenced VOICES' innovative approach to providing information, a wide range of longterm support services, and commemorative events for those impacted by 9/11. In 2006 VOICES launched the 9/11 Living Memorial Project, a digital archive that includes over 70,000 photographs and personal mementos documenting the nearly 3,000 lives lost and stories of survivors. A strong proponent for victims' families, Ms. Fetchet advocated for numerous 9/11 issues as well as the creation of the 9/11 Commission and reforms based on their recommendations. Ms. Fetchet testified before the 9/11 Commission and US Congress on five occasions.

Her work has received national recognition including the 'Connecticut Hero' award by Senator Joseph Lieberman, ABC News Person of the Year, and NBC News Making a Difference. Most recently, Ms. Fetchet was inducted into the Hall of Fame at Columbia University School of Social Work in NYC. VOICES is currently completing a Resource Kit to assist organizations and communities responding to acts of mass violence. The Resource Kit is based on extensive scholarly research and interviews with those who responded to the Oklahoma City bombing, the 9/11 attacks, shootings at Virginia Tech, Northern Illinois University and Tucson, Arizona. With offices in Connecticut, New Jersey and Washington, DC, VOICES intends to support other communities in preparing for, responding to and recovering from acts of mass violence.

Michael T. Flynn,
Lieutenant General
Director
Defense Intelligence Agency

Mr. Lieutenant General Michael T. Flynn graduated from the University of Rhode Island in 1981 and was commissioned a second lieutenant in Military Intelligence. His first assignment was as a paratrooper of the 82nd Airborne Division at Fort Bragg, North Carolina. Since that time he has served in a variety of command and staff positions to include, Commander, 313th Military Intelligence Battalion and G2, 82nd Airborne Division; G2, 18th Airborne Corps, CJ2, CJTF-180 Operation Enduring Freedom (OEF) in Afghanistan; Commander, 111th Military Intelligence Brigade at the Army's Intelligence Center at Fort Huachuca, Arizona; Director of Intelligence, Joint Special Operations Command with duty in OEF and Operation Iraqi Freedom (OIF); Director of Intelligence, United States Central Command with duty in OEF and OIF; Director of Intelligence, the Joint Staff; Director of Intelligence, International Security Assistance Force-Afghanistan and US Forces-Afghanistan, Special Assistant to the Deputy Chief of Staff, G-2, and Assistant Director of National Intelligence, Partner Engagement. LTG Flynn became the 18th Director of the Defense Intelligence Agency on 24 July 2012.

Lieutenant General Flynn also served in several other Army, Joint, Interagency and Coalition assignments over his distinguished career. Additionally, he has authored numerous professional journal articles on national security, and defense related issues. LTG Flynn is also the recipient of the distinguished Association of Special Operations Professionals Man of the Year Award for 2012.

Neil Gaughan
Assistant Commissioner, National Manager Counter-Terrorism

Neil Gaughan joined the Australian Federal Police (AFP) in 1984 working in a variety of general policing and investigative roles in the ACT Region prior to transferring to the National Internal Investigation area in 1998. In late 1999 Neil left the AFP and joined the Australian Taxation Office working in the investigations, fraud control planning and risk management fields.

In 2004 Neil returned to the AFP and worked in the Protection portfolio being promoted into the role of Manager Close Protection, in 2005. Whilst in Protection Neil had responsibility for the AFP's close protection activities as well as the national witness protection program and delivered AFP outcomes for APEC 2007 and World Youth Day 2008.

In August 2008 Neil transferred to High Tech Crime Operations (HTCO) and in December 2009 was promoted to National Manager. In HTCO Neil led investigation teams with responsibility for all complex cyber-crime and online child exploitation investigations, as well as delivering all the AFP's technical, interception and surveillance capabilities.

In 2013 Neil took over responsibility for the Counter-Terrorism (CT) portfolio. The CT function provides the AFP with the ability to prevent, disrupt and investigate terrorist activity against Australia and Australian interests both domestically and internationally.

Gordon Graham
President
Lexipol

Gordon Graham is a retired 33 year veteran of California Law Enforcement. During his tenure as a police professional, he was awarded his Teaching Credential from California State University, Long Beach. He later graduated from University of Southern California with a Master's Degree in Safety and Systems Management. Subsequent to this he graduated from Western State University with a Juris Doctorate.

Mr. Graham has taken this background as a street cop, supervisor and manager and coupled it with his formal education as a risk manager and his education and experiences as an attorney and is now President of Lexipol – a company designed to standardize policies, procedures and training within law enforcement agencies around America.

Over the last decade, Mr. Graham has spoken to over 300,000 law enforcement and other public safety professionals from every State in the country, no doubt some from your Department. He has traveled extensively overseas delivering his message regarding improving the quality of law enforcement operations.

In 1995, Mr. Graham received the Governor's Award for Excellence in Law Enforcement Training, the highest tribute available in the critical mission of training police professionals. In 2008 he received the lifetime achievement award from California POST.

Susheel Gupta
Air India Victims' Families Association

Susheel Gupta is on leave from the Public Prosecution Service of Canada. Prior to his current position he worked with the Department of Justice War Crimes Section while a majority of his career has been spent as a Federal Prosecutor and Computer Crime Advisor.

With respect to National Security and Intelligence issues, Susheel was one of the prosecutors in Canada's first prosecution under the Anti-Terrorism Act. On a more personal note, Susheel has been actively involved in issues of national security, terrorism and security. He was 12 years old when his mother was murdered when Air India Flight 182 exploded with a bomb on board. She was only 37 at the time. Since that tragic day, he has been a spokesperson for the Victims' Families Association. He was one of the key individuals who fought for a full Public Inquiry into the Air India Bombing. It was this terrorist incident and tragedy that led him to his career path in serving the public. Susheel brings a unique and diverse background on issues that are relevant to all of us and offers many perspectives due to his security and justice system expertise and experience as a victim of terrorism.

Michael Haley
Sheriff Washoe County Sheriff's Office, Reno, Nevada

Sheriff Haley was elected November 2006 taking office January 2007. He has served the Washoe County Sheriff 's Office for 33 years. He was elected to a second term on January 2011 and ran unopposed. He is only the second Sheriff in over 64 years to be promoted through the ranks and assume leadership of the Sheriff 's Office. His career assignments include Instructor Police Academy, Assistant Staff Officer to the Sheriff, homicide and property crimes command as well as hostage and special weapons team command.

Since taking command of the Sheriff 's Office, Sheriff Haley has created the Area Crime Evaluation System (ACES), AlertID an automated computer-driven public crime alert system, iWebvisit system and the Cyber Crimes Unit.

In addition to his duties as Sheriff, he serves as Vice-Chair for the Nevada Commission on Homeland Security, Chairman of Nevada High-Intensity Drug Trafficking Area program, President of Nevada Sheriff 's and Chief's, Chairman of the State of Nevada Network responsible for building the nationwide LTE network and Board of Directors for Leadership in Counter-Terrorism Alumni Association.

Michael Julian
General Manager, Security for Westfield Australia

Michael is a New Yorker who relocated to Sydney, Australia in 2005 to assume the role of General Manager, Security for Westfield Australia. He has worked closely with the NSW Police Force to prevent crime and respond to the terrorism threat. He commanded specialized police divisions, including Policy, Training and Public Information. He coordinated the Community Policing effort, managed the Legal Bureau and commanded the police response to the most volatile demonstrations and civil disorders.

Before his retirement as Chief of Personnel, Michael was part of Police Commissioner Bill Bratton's senior leadership team that reduced crime by 30% in two years and started a world-wide renaissance in crime prevention.

After leaving the NYPD, Michael became a Senior Vice President at Rockefeller Centre responsible for Protection and Public Services. He then served for nearly four years as General Manager of Madison Square Garden, leading the team that produced NY Knicks basketball games, NY Rangers hockey games and concerts.

Michael's education includes a Bachelor's, a Master's and a Law Degree, as well as a Management Diploma from Columbia University. He is passionate about reducing crime, creating safe cities around the world, and rooting for the Brooklyn Nets.

Michael Leiter,
Senior Counselor
Palantir Technologies

Michael Leiter is the Senior Counselor to the CEO of Palantir Technologies. Prior to entering the private sector Leiter served as the Director of the National Counterterrorism Center (NCTC) until July 2011. He was sworn in as NCTC's second-ever Director on June 12, 2008, upon his unanimous confirmation by the U.S. Senate and after serving as the Acting Director since November 2007. He was initially nominated to serve as Director by President George W. Bush in March 2008.

Before joining NCTC, Mr. Leiter served as the Deputy Chief of Staff for the Office of the Director of National Intelligence. Prior to his service with the ODNI, Mr. Leiter served as the Deputy General Counsel and Assistant Director of the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. From 2002 until 2005 he served as an Assistant United States Attorney.

Mr. Leiter received his J.D. from Harvard where he graduated magna cum laude and was President of the Harvard Law Review, and his B.A. from Columbia. He is a member of the RAND Corporation Board of Trustees, the National Security Agency's Advisory Board (Cyber Awareness and Response), the NCTC Director's Advisory Board, the Bipartisan Policy Center Homeland Security Project, the Aspen Institute's Homeland

James Malizia
Assistant Commissioner Federal Policing Operations Royal Canadian Mounted Police

Assistant Commissioner James Malizia is responsible for Federal Policing Operations, which includes the oversight of investigations in relation to terrorism, serious and organized crime, and financial crime. In addition, he oversees protective policing, security for major events, and the Canadian Air Carrier Protective Program.

Throughout his career, Assistant Commissioner Malizia has worked as an investigator where he has successfully led several national and international organized crime investigations and proceeds of crime operations, targeting Colombian cartels, traditional organized crime groups, outlaw motorcycle ganga and street trafficking and money laundering.

As a Commissioned Officer, he has also directed investigations into corruption, fraud, immigrations, contraband tobacco, terrorism and serious organized crime. These major investigations include "Project Colisee" which resulted in the successful dismantling of a significant transnational organized crime group.

In 2006, he completed the Canadian Police College's Executive Development Program where he was awarded the Student Award of Excellence. He is also a graduate of the Leadership in Counter-Terrorism Program and is currently in the process of completing a Master's of Leadership and Management with Charles Sturt University.

Brain MacDonald
Inspector Professional Standards
South Coast British Columbia
Transportation Authority Police Service

With over 34 years of policing experience Brian MacDonald is in charge of the Professional Standards Unit of the Metro Vancouver Transit Police.

Brian has served the Transit Police as interim Chief, Operations Officer and Acting Deputy Chief. In 2010 Brian retired from the Royal Canadian Mounted Police having served in Drug Enforcement, Patrol, Major Crime, National Security Enforcement and the 1985 Air India Disaster Task Force. He is a LinCT program alumnus from the 2005 Atlantic program.

Celia Mathieson

Celia Mathieson has worked in various roles within the United Kingdom's Counter Terrorism structure for over 15 years. Since 2005, she has worked within the CT Police network, initially in Scotland, during the G8 Conference in 2005 and the attack on Glasgow Airport in 2007.

However since 2009 she has worked within the Metropolitan Police SO15 - in particular, contributing to the planning for and delivery of the L2012 Olympics CT machinery. She graduated through the LinCT program in 2006 and continues to work daily with many of the contacts she made through LinCT.

Philip Mudd
Director of Global Risk
Southern Sun Asset Management

Philip Mudd joined the Central Intelligence Agency in 1985 as an analyst specializing in South Asia and then the Middle East. He began work in the CIA's Counterterrorist Center in 1992 and then served on the National Intelligence Council as the Deputy National Intelligence Officer for the Near East and South Asia (1995-98). He later managed Iraq analysis at the CIA (1999-2001). Mr. Mudd worked on Middle East issues at the White House National Security Council in 2001 and left after the September 11 attacks for a short assignment as the CIA member of the small diplomatic team that helped piece together a new government for Afghanistan.

He returned to the CIA in early 2002 to become second-in-charge of counter-terrorism analysis in the Counterterrorist Center. He was promoted to the position of Deputy Director of the Center in 2003 and served there until 2005, when FBI Director Mueller appointed him as the first-ever deputy director of the National Security Branch in 2005. He later became the FBI's Senior Intelligence Adviser and then resigned from government service in March 2010. Mr. Mudd has commented about terrorism often in Congress, and he has been featured by ABC, NBC, CBS, CNN, Fox, BBC, MSNBC, al-Jazeera, NPR, the New York Times, and the Washington Post. Mr. Mudd has written in Newsweek, the Wall Street Journal, The Atlantic, Foreign Policy, the Washington Post, and Sentinel, the journal of the US Military Academy's Combatting Terrorism Center. He now serves as Senior Global Adviser to Oxford Analytica, a British-based firm specializing in advising multinational companies. He sits on the Aspen Institute's Homeland Security Group and is on the advisory board of the National Counterterrorist Center.

Sue O'Sullivan
Federal Ombudsman for Victims of Crime

Sue O'Sullivan, a 30 year law enforcement veteran and former Deputy Chief of Police for the Ottawa Police Services, began her term as Canada's Federal Ombudsman for Victims of Crime August 16, 2010.

Throughout her law enforcement career, Ms. O'Sullivan has served in Patrol, Criminal Investigative Services and Operations Support. Ms. O'Sullivan is a member and past President of the Leadership in Counter Terrorism Alumni Association (LinCT AA), a group of senior professional executives who work together to influence local, national and international counter terrorism strategy, and has acted as an advisor to the Auditor General of Canada on National Security in Canada –The 2001 Anti- Terrorism Initiative Audit.

Throughout her career, Ms. O'Sullivan has continually advocated to increase the efficiency of services to victims. Prior to her appointment, Ms. O'Sullivan worked with stakeholders from the victim services community and all three levels of government to develop a coordinated victim assistance program.

Ms. O'Sullivan has been recognized for her leadership both within the service and in the community. Her honors include the Governor General's Officer of the Order of Merit of the Police Forces Award, the Queen's Golden and Diamond Jubilee Medals, the Governor General's Exemplary Service Medal, the YWCA Women of Distinction Award, the St. Joe's Women's Centre Quality of Life Award, and the Circle of Canadians Community Service Award.

John Parkinson OBE, M. St. (Cantab), Comp. I.M.S.

John served with West Yorkshire Police, which is the 4th largest police force in the UK for over 33 years before retiring in March 2013 as the Chief Constable. His career centered on criminal investigation with specialisms in homicide, kidnap and extortion, organized crime enquiries and counter terrorism. He attended the Counter Revolutionary Warfare and Insurgency module of the British Military Command Course in 1996 and became and accredited Association of Chief Police Officers Counter Terrorism Senior Investigating Officer in 2004.

With colleagues from the Metropolitan Police, he oversaw the investigation in Leeds into the 7/7 London Bombings and subsequently led the review to increase capability and capacity in counter terrorism and established the first North East Counter Terrorism Unit. He has been the Gold Commander on many varied Counter Terrorism Operations and led on many national CT Exercises. He performed the role of UK Senior National Coordinator Counter Terrorism becoming Chief Constable in West Yorkshire Force in the UK. He was a Vice President of the Association of Chief Police Officers Terrorism and Allied Matters Committee before retirement.

John was awarded the OBE by Her Majesty the Queen for his services to Policing and Counter Terrorism in 2011. He holds a Masters Degree (with Distinction) from Cambridge University in Applied Criminology and is a Companion of the Institute of Management Specialists. He is also a graduate of the International Leadership in Counter Terrorism Programme (LinCT) and was President of the Alumni Association in 2008.

Michael Peirce
Assistant Director, Intelligence
Canadian Security Intelligence Service

As Assistant Director Intelligence, Mr. Peirce reports to Director and is responsible for the assessment and dissemination of intelligence including strategic intelligence and raw intelligence reports. As CSIS is an intelligence led organization, Mr. Peirce is also responsible for setting the intelligence collection requirements for the Service.

Mr. Peirce joined CSIS from the Department of Justice Canada (DOJ) where he was the Deputy Executive Director and General Counsel with the CSIS Legal Services.

He has worked in the national security field throughout his career in government, including representing the Service before courts and tribunals and as the Lead Counsel for the Government of Canada during the inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin.

Mr. Peirce worked in a variety of positions at the DOJ. He spent three years as the Director of Legal Operations at the Privy Council Office. Mr. Peirce has also taught Comparative Constitutional Law and Legal Research and Advocacy as an associate at Columbia University and lectured at University of Ottawa and Carleton University.

Mr. Peirce has a BA from the University of Toronto and LLB from the University of Western Ontario, an LLM from the University of Wisconsin and an LLM from Columbia University.

John S. Pistole
Administrator
Transportation Security Administration

John S. Pistole was confirmed as the Transportation Security Administration's (TSA) fifth Administrator in July 2010. As TSA Administrator, he oversees management of a 60,000-strong workforce, the security operations of 450 federalized airports throughout the U.S., the Federal Air Marshal Service (FAMS), and the security for highways, railroads, ports, mass transit systems and pipelines.

Pistole came to TSA as a 26-year veteran of the FBI. After the tragic events of September 11, 2001, he was put in charge of the FBI's counter-terrorism program, eventually becoming the FBI's Executive Assistant Director for Counterterrorism and Counterintelligence. In 2004, Pistole was named Deputy Director for the FBI.

His experience includes several high profile investigations, including the attempted car bombing in Times Square on May 1, 2010; the December 25, 2009, attempted attack on Northwest Flight 253; the plot against New York City subways in 2009; the 2006 UK liquid explosives plot; and the May 2003 suicide bombings in Riyadh, Saudi Arabia, in which 35 people died, including nine Americans.

Pistole practiced law for two years prior to joining the FBI. He is a graduate of Anderson University (Indiana) and Indiana University School of Law – Indianapolis. He is married and has two daughters.

Michael Richards
Deputy Director Intelligence
New Zealand Security Intelligence Service

Michael (Mike) Richards was born in Sydney on 30 June 1954 and grew up in Adelaide and Melbourne.

Mike graduated from Monash University in Melbourne (Bachelor of Jurisprudence, 1975 and Bachelor of Law, 1978) and joined the Australian Security Intelligence Organization (ASIO) in January 1979. He progressed through operational and analytical postings mainly focusing on extremism sourced in or from the Middle East and between1986-1988, served as an exchange officer with the United Kingdom Security Service. He then served in ASIO's Central Office in Canberra and ASIO's Sydney office before returning to Canberra in 1995.

He resigned from ASIO in 2000 to take up a job as a fraud and corruption investigator with the World Bank's Department of Institutional Integrity. While based in Washington DC, he travelled extensively to Bosnia, Indonesia, Philippines, Timor-Leste, Vietnam and India. Mike re-joined ASIO in September 2007 as a Branch Manager initially in Canberra but moving to Sydney in July 2008 to head ASIO's CT investigations in that city.

From late January 2011, Mike commenced a three year secondment as Deputy Director Intelligence with the New Zealand Security Intelligence Service. Mike has a 26 year old daughter from a previous marriage and re-married in November 2011. His keen interest is in military history especially naval history and has ambitions to research and, if possible, publish on colonial fortifications in Australia.

Irfan Saeed
Senior Policy Advisor
US Department of Homeland Security
Office of the Secretary, Office for Civil Rights and Civil Liberties

IrIrfan Saeed currently serves as a Senior Policy Advisor, in the US Department of Homeland Security, Office for Civil Rights and Civil Liberties. Mr. Saeed advises DHS leadership on policy issues at the intersection of civil rights and homeland security, developing and coordinating activities relating to countering violent extremism. Prior to joining Homeland Security, Mr. Saeed worked as a criminal prosecutor, at the state and federal level. Mr. Saeed worked as an Assistant United States Attorney, US Department of Justice, in the Eastern District of Louisiana, as well as an Assistant District Attorney, in New Orleans, Louisiana.

During his federal employment, Mr. Saeed has also worked extensively overseas. He served as the Resident Legal Advisor in two US Embassies-in Tashkent, Uzbekistan, and Bishkek, Kyrgyzstan.

In addition, while deployed to the US Embassy in Islamabad, Pakistan, he was tasked to develop the Community Engagement Office, the first of its kind in U.S. Embassies worldwide, to use traditional public diplomacy tools to counter violent extremism (CVE) in Pakistan.

Mr. Saeed is a graduate of the Federal Bureau of Investigation (FBI) Academy, College of Analytical Studies, Quantico, Virginia; Loyola University School of Law, and Louisiana State University.

Jim Stokley
Detective Superintendent
Counter Terrorism Command New Scotland Yard

Jim joined the Metropolitan Police in 1993 becoming a Detective in 1999 on the Homicide Command. Promoted in 2001 he moved to Brent Borough leading their sexual offenses team. In addition to investigations he created and led a crime prevention campaign, winning an advertising industry award, raising awareness of rape in minicabs, leading to crime reduction and the London wide licensing of minicabs.

In 2002, as a Detective Inspector, he established the Cold Case Rape Team, utilizing enhanced DNA techniques to identify suspects. This pioneering work had a 100% conviction rate.

In 2004, he joined the Anti Terrorist Branch and currently leads a number of teams responsible for investigating terrorist offenses in the UK and overseas. He has successfully convicted terrorists for the kidnap of UN workers in Afghanistan, the training and operational support to the perpetrators of the Casablanca and Madrid bombings and created and led the CCTV team playing a pivotal role in investigating the bombings of London. He led the UK response to the attack in Algeria.

During his service, he has been commended eight times including to the Commissioner for his work during the London Bombings.

Stuart Thorn
Deputy Director- General

Mr. Thorn joined the Organization in 1985. He is a career intelligence officer and has worked in a range of analytical and operational roles, with a focus on counter-terrorism. He has managed the Organization's Middle East analytical area as well as a range of operational areas.

He was appointed a Senior Liaison Officer to Washington in 1993 and was responsible for the exchange of intelligence with key U.S. and Canadian intelligence and Law Enforcement partners.

In 1997, he was promoted into the Senior Executive Service and assumed management of activities in NSW, Queensland and the Northern Territory. This included the management and execution of intelligence operations to protect the 2000 Sydney Olympics and the aftermath of 9/11.

In 2003 Mr. Thorn was promoted to head of Technical and Surveillance Divisions and in 2006 was promoted to Deputy Director- General, responsible for oversight of all analytical and operational capabilities and resources.

Justin M. Vallese
Supervisory Specialist, Cyber
Program Coordinator
Federal Bureau of Investigation

Justin M. Vallese is an FBI Supervisory Special Agent for a cyber-national security computer intrusion squad comprised of Special Agents, Intelligence Analysts and a computer scientist. This squad is responsible for conducting counter-terrorism, counterintelligence and criminal cyber investigations which affect the greater Los Angeles area.

As Cyber Program Coordinator for the Los Angeles FBI Cyber Branch, SSA Vallese also works with the Electronic Crimes Task Force in various computer intrusion investigations and intellectual property theft matters. Prior to his work in the cyber arena, SSA Vallese was assigned to working Financial Crime investigations at the FBI Los Angeles.