



Intelligence-Informed Decision-Making to Build a More Secure Future



Hosted by the
Tom Ridge School of
Intelligence Studies and
Information Science
At
Mercyhurst University

Dungarvan, Ireland

12 July - 15 July 2015

Table of Contents

Introduction	2
Keynote Speaker – Noirin O’Sullivan – Commissioner of the Garda.....	3
Questions for Noirin O’Sullivan	4
Plenary Session.....	5
The Honorable Howard Schmidt: Keynote	7
“GIF” Talks – Paul O’Doircuide and Benedict O Floinn	9
Cyber Security Panel	10
Anticipatory Intelligence Panel	11
Intelligence Trends Panel.....	11
Keynote Speaker – Lew Merletti	13
A Wicked Approach to Intelligence	15
Conclusion	17

Introduction

Mercyhurst University's Institute for Intelligence Studies hosts the bi-annual Global Intelligence Forum in Dungarvan, Ireland. The theme for the 2015 forum was "Intelligence-Informed Decision-Making to Build a More Secure Future."

The forum in accordance with the University's holistic approach to the field of intelligence, centered on building bridges between decision-makers, practitioners and scholars in the fields of cyber security intelligence analysis, law enforcement, business and data analytics. Best practiced panelists also addressed the themes of anticipatory analytics, and the wicked problem approach to intelligence challenges. Additionally, the forum provided a higher education breakout session for leaders to discuss the application of intelligence practices to higher education decision making. The forum aimed to bring best practices in 21st century intelligence and data management to both public and private sector leaders and explore what is required to make more effective decisions.

Keynote speakers included Noirin O'Sullivan, Commissioner of the Garda, Ireland's National Police Service, Lewis Merletti, Former Director of the U.S. Secret Service, and the Honorable Howard Schmidt. For the first time, the forum introduced "GIF talks", with two separate segments; the first by Paul O'Doircuide, intelligence specialist, and the second Benedict O' Floinn, Attorney at Law. In addition to two higher education breakout sessions, Jim Breckenridge, Dean of the Tom Ridge School of Intelligence Studies and Information science; Steve Zidek, Assistant Professor of the Tom Ridge School of Intelligence Studies an Information Science; Melonie Richie, Deputy Director of Camber Corporation; and Kathleen Moore, professor of Intelligence Studies moderated panels on the following topics:

- ❖ Cyber Security
- ❖ Anticipatory Intelligence
- ❖ Intelligence Trends
- ❖ A Wicked problem approach to Intelligence
- ❖ Intelligence in Higher Education

This document contains an overview of the conference.

For more information, please contact:

Michelle Henderson
mhenderson@mercyhurst.edu
(814) – 824 – 2131

Keynote Speaker – Noirin O’Sullivan – Commissioner of the Garda

The theme of Noirin O’Sullivan’s Speech involved the relationship between intelligence and the decision maker... and how to expand to a larger understanding of intelligence.

Noirin spoke about the environment of policing and intelligence in Ireland. The official name of the police force “Guarda Siochana” means “the guardian of the peace.” The Garda is entirely unarmed force, which important to keep in mind when discussing the dynamic of the Garda and how it functions. The country has a dual mandate of policing and security, so as commissioner the Garda, O’Sullivan is head of policing but also head of security and intelligence. This means safely and peacefully protecting the people, while combatting terrorism, an indigenous threat of the island of Ireland.

On this Noirin talks about 4 main points:

- ❖ Intelligence as an ever changing field: In this ever globalizing world, O’Sullivan says what is great for trade and the economy poses a “*unique challenge for intelligence service.*” People are using social media to radicalize at home. It used to be plausible to figure out who was working together. Everything was hierarchical, with a leader, and members with roles and responsibilities. Now the threat is displaced. Anything can happen at any given time. “*It’s about how to know what you don’t know that is a huge issue.*” She also added: “*Complacency is dangerous... if we think we are in a good place, then we are not a head of the curve.*”
- ❖ Community: As a police and intelligence service, it is important to work for, but also work WITH the community. “*Triangulate the intelligence and contextualize it back into the community.*” There needs to be a strong element of trust in the community, which will enable front line engagement. “*It is the connectivity that allows us to contextualize that intelligence.*”
- ❖ Intelligence’s role in decision making: “*I want to make sure my decisions are informed decisions and evidence based decisions... we need to present not statistics, but evidence based analytics.*” When describing what is needed in an intelligence analyst... O’Sullivan said “*We need people who can discern patterns in the data, are good story tellers, then can answer the question I have, present it in a nice way, and make recommendations on the best practice.*”

- ❖ Paralysis by Analysis: O’Sullivan discusses the fear where blame, in retrospect, may be placed on the analyst OR the decision maker. If the analyst or decision maker is a risk averse person, they may be more likely to not recommend (or take) an action. So, it becomes important there is a set framework through which analyst work, or else all the analyst and potential outcomes of a situation may freeze an analyst. It needs to be determined who is responsible for intelligence that is unsanctioned. *“Intelligence unsanctioned is the highest risk we gather... If [intelligence] is to be of real benefit... it has to be presented in an actionable format, there needs to be clear format of ownership and who is responsible for action in this intelligence.”*

She ends with the quote: ***“Put together the best minds the best will to make it happen, we can make a difference for the future.”***

Questions for Noirin O’Sullivan

- ❖ A question from an attendee addresses **drug related crime, and whether in-reach or out-reach was the most favorable to investigating and stopping the illegal activity.** O’Sullivan responded that “It is best to have both” and explained how they reach out to key influencers in communities in Ireland, but also have ethnicity liaison officers and integrated education in communities. *“It’s about making sure that people have a shared sense of community... balancing the in reach and outreach”*
- ❖ A question was asked about **how to train for intuitive decision making,** using the example of going through 15 steps of an informed decision in 11 seconds. O’Sullivan responded that the training must involve a lot of solution focused problem solving. She explains the importance of training how to innately go through the proper steps, while weighing in accountability. Train to be proper, appropriate, legal, and with necessary justification, but also taking into account that *“there are consequences when people become paralyzed by fear and don’t take action.”*

Plenary Session

Panelists: Jim Breckenridge (moderator), Mike Barton, Frank Daly, David Dausey, Andrew Roth, and Dale Watson

Collectively, after Noirin O’Sullivan set the tone of the day, the panelists addressed the issues set forth in the panel themes, focusing on how intelligence effects their respective fields of work.

- ❖ Mike Barton, Chief Constable of county Durham as well as head of intelligence for England, explained how England has made advances in the system using technology. There now is a cross national database including every bit of crime intelligence, arrest record, from every town in England. Additionally body worn cameras are on at all times live streaming, and an Intelligence Professionalism Program has been set in place. According to Barton, there needs to be an “*up-for-it-ness*” in the policing and intelligence culture to try new things and make advances.
- ❖ Frank Daly, chairman of the board of NAMA explains that “*evidence based decision making is the only way NAMA can function.*” Using the Business Intelligence model, NAMA has been able to capture key messages from unstructured market intelligence, stop trend and changing dynamics, matching operational intelligence with market intelligence and much more. Ultimately NAMA lowered Ireland’s debt from 32 billion to 18 billion.
- ❖ David Dausey stated “*Making an informed decisions comes down to having the right data and analyzing it properly*” and discusses the information conundrum that so many professionals face today. There is endless data, too much data, which can be collected compiled analyzed, but unless it is USED, you will get in trouble according to Dausey. Rare events such as in combating terrorism or a public health outbreak are hard to prepare for and hard to learn from.
- ❖ Andrew Roth set the tone of his session by saying “*work smarter not harder.*” Discussing the possibility of the creation of a new discipline, he asks “*when does one discard intuitive and experience based decision making and adopt information based decision making?*” (In regards to running a higher education institution). An extensive list of possibilities include maximizing learning outcomes of students by using intelligence based decision making,

course development using intelligence, and how to be mission sensitive but market smart.

- ❖ Dale Watson discussed how intelligence analyst always were getting second guessed post 9/11... due in part to the clarity post event. The scrutiny of analyst and decision makers' post 9/11 caused everyone to be very cautious about what recommendations were made. Today, the modern analyst is cautious, but Watson expresses the need for a different type of people. We need people "*well educated who have the ability to understand data, search, and use social media...*" and explains they need to come from a variety of places because you want a wide demographic of people with different backgrounds, to have a holistic understanding of the question at hand.

The Honorable Howard Schmidt: Keynote

The Honorable Howard Schmidt used a question and answer format for his segment. The questions and preceding answers are summarized below:

Questions 1: Can you speak to the aggressive nature of state and non-state actors, including but not limited to inadequacies and vulnerabilities?

- ❖ “[The U.S. Government] could kick butt with what we know, but we are not allowed to implement [action]” Leaders look at policy but aren’t allowed to implement it, and the people implementing don’t have a say.

Question 2: Can you talk about a time when you had issues with policy and policy implementation?

- ❖ In summary, Schmidt explains the difficulties of timeliness as “*the government works at government speed, the rest of us work at internet speed,*” and trying to work as a moderator to give private industry the ability to protect themselves. The weighing between government, commercial, and private intelligence can cause an interesting policy issue. A unified solution was hard to come by.

Question 3: How can market mechanisms both promote and detract from cyber security?

- ❖ Explain a weakness, Schmidt stated that the private sector owns and operates what we consider critical infrastructure, and there was no organization in the government set to deal with it. The private sector didn’t have the ability to protect themselves, or talk to one another and learn from mistakes, which meant the critical infrastructure really didn’t have protection. This realization led to the development of ISAC information Sharing and Analysis Centers (ISAC) as a solution to the problem. ISAC’s serve to share information between public and private entities.
- ❖ Additionally, regarding the National Strategy to Secure Cyber Space, and weaknesses in cyber security, Schmidt comments – “*We wind up in a situation where we are really good at identifying the problem, getting a group of qualified people together to talk about it, and it stops there.*”

Questions 4: What is the most vulnerable infrastructure?

- ❖ Government operations

- ❖ Power sector
- ❖ Financial Services
- ❖ Telecommunications

Question 5: What is an act of war in this cyber environment?

- ❖ To this question, Schmidt jokes “Are there any Attorneys in the room?” After much speculation concluded that it would depend on who it is and what their intentions are.

Question 6: Much of the past cyber issues have involved shutting down of system... but what about the compromise of systems? For example the FBI finger print system? Has there been research into the protection of systems such as that?

- ❖ Availability, and confidentiality with information and systems are good, but “*integrity is the wild card.*” Integrity within both the government and the private sector is an issue.

Question 7: In your travels, what do you see as the greatest weakness?

- ❖ Schmidt replied that it is the competing equities that cause weakness. In law enforcement, there is not cut and dry rules saying who responds to what, and in some cases cyber is not seen as a priority. Additionally, there are not enough people with the necessary training to handle all the situations ongoing.

Question 8: We know breach companies rarely discover a breach right away... why does it take so long, if you do have a cyber-incident, what should be the plan?

- ❖ Speaking to this issue, Schmidt reinforces that 99% of people have no idea what is going on or how to fix it... so you must demand the manufacture follow all best practices and follow up with the people running the program at the company.

Question 9: What do you see as disruptive technology in the cyber realm, in terms of offenders and defenders?

- ❖ Cryptology and encryption. The private sector needs to be more open to the idea of allowing government access to their data to protect everything.
- ❖ Quantum Computing

“GIF” Talks – Paul O’Doircuide and Benedict O Floinn

Mr. Paul O’Doircuide spoke on the topic of the Darknet, bitcoin, and cyber-crime. These are topics that many often hear about, but rarely see or comprehend. Main points included:

- ❖ The Darknet is inaccessible through regular browsers, you need a tor browser. (Downloadable at torproject.org) Tor browser includes layers of encryption, and allowing the user to easily change identify at any point with the click of a button.
- ❖ You can buy counterfeit money, credit cards, packages including an entire person’s identity, drugs, cigarettes, guns, anything illegal on the Darknet, just like eBay.
- ❖ Most all of the financial transactions happen through Bitcoin, which is intentionally designed to be anonymous.
- ❖ A new trend emerging is the sale of services on the Darknet, such as offering to shut down sites, for a cost.
- ❖ Ethereum is service allows for complex contracts to be uniquely designed for someone’s specific needs, it is all autonomous and self-executable within the Darknet environment, with anonymity and no need for a third party.

Mr. Benedict O Floinn talks about the difficulty in handling the unique dynamic of the cyber security world. Some major points included:

- There is so much data, so many cases regarding cyber-crime, O Floinn stated, *“It is simply a self-defeating object because we can never catch it.”*
- We need to find the tangible within the cyber world in order to harness the traditional laws and apply them to cyber-crime.
- Digital natives are entering the work force. O’Floinn expressed his concern over need to preserve the value of challenging everything, including what is seen on a computer screen, as digital native don’t inherently do this.
- We can have as much information as you want, but, as law enforcement officials would know, *“a case is only as good as the reliability of the information and the person who is putting the information together.”*

Cyber Security Panel

Panelists: Steve Zidek (moderator), Bob Hayes, Srinivas Kumar, Jaroslav Jakubcek, James Emerson

Bob Hayes:

- ❖ Citadel Bonnet exemplifies why criminals love cyber. The criminals behind the act made 500 million and no one was prosecuted.
- ❖ There is data where you may least expect it. The Power BI plug in on Excel is an excellent way to look at data in a different way.

Jaroslav Jakubcek:

- ❖ Cyber Criminals use legitimate and legal software to aid in their crimes, such as Tor, IRC, Jabber, bitcoin.
- ❖ Tool kit and Bit-talker are encryption keys.
- ❖ There is somewhere around 1.2 billion USD in the Darknet
- ❖ Jakubcek concludes by warning that to tackle this cyber-crime underground is near impossible because of the decentralization of control.

Srinivas Kumar:

- ❖ Big data is a problem we created because we mine a lot of data. "Data without context is noise. Data with context is evidence."
- ❖ On data and policy: "If you don't know why to monitor, no policy will help you. If you don't know how to discover, no process will guide you there. If you don't know what to measure, no metric will take you there."

James Emerson:

- ❖ Regarding cyber entities and how to protect them, Emerson said "we understood the threat and risk, but no one knew how to do anything about it"
- ❖ In law enforcement, cyber requirements are increasing. Digital evidence are increasingly required, crimes have a cyber-element
- ❖ "Until we can communicate at machine speed we will never produce preventative intelligence"
- ❖ Development of ISAO (Information Sharing and Analysis Organizations)

Anticipatory Intelligence Panel

Panelists: Melonie Richie (moderator) Kevin M. O’Connell, Bill Richardson, Abe Usher

I HAVE NO NOTES FOR THIS PANEL

Intelligence Trends Panel

Panelists: Kathleen Moore (moderator), John Goldener, Aidan Connolly,

John Goldener:

- ❖ Reflecting on the past few years, trends that have stood out are the large growth in size of budgets and size of programs. People are staying longer. We used to see people coming out of government into private sector, and then back into government, now people are making the private sector intelligence a career.
- ❖ *How do you maintain high quality analysis while keeping products short?*
- ❖ Overall the quality of analysis is going up. Analysts hold more degrees and many are bi-lingual. Demographic trends show analysts getting younger, and in manager and leadership roles by age 30-39. By gender, the intelligence community is split almost 50% male 50% female, but mostly white.
- ❖ Lack of strong customer feedback still remains
- ❖ The role of the analyst is changing. *A really strong analyst is going to have to be the tool master. They don’t need to have every skill, but they need to know who does have the skill. The skills that are going to be critical are creative thinking and intuition.”*

Aidan Connolly

- ❖ The three reasons why analytics fail all involve people, *“as people are intelligence’s greatest strength and Achilles heel.”*
 - Deception or inexperience of the customer, including ignorance and not really know what intelligence you are buying or how to use it.
 - Analytics ... or alchemy?
 - Failure of person to change the behavior after receiving intelligence.
- ❖ Analytics helps see the world as it is, not as one would wish it would be.

Kathleen Moore

Moore discussed the rise of the citizen analyst, looked at through a social media context.

- ❖ Social media brought about hunters and gathers of intelligence during big events or crises such as natural disasters. This was first noted in Hurricane Katrina when people took to wiki to do their own reporting and develop a communication infrastructure.
- ❖ Other examples include the Virginia Tech massacre, California Wildfires, the earthquake in Haiti, and so many more, all where civilians were taking to social media to share and discover information.
- ❖ How do we vet and analyze this information?
- ❖ Trends have shown that these people are empowered and self-organized, and simply concerned citizens. They vet each other for reliability... *“in these peoples’ minds, deception and trust are just opposites”*
- ❖ During crisis events people come together regardless of culture or country... and social media serves as the homogenizer.

Keynote Speaker – Lew Merletti

Lew Merletti began his speech by explaining how he found himself in the Intelligence field in the first place, taking listeners back to 1966, when he heard Kennedy call to the people of America “ask not what your country can do for you but what you can do for your country.” It was then he decided to enlist in the U.S. Army and found himself on his way to Vietnam. Merletti moved through ranks with ease, graduating basic training and then paratrooper school, then special forces in a cross training program as a Vietnamese interpreter and medic.

Reflecting on lessons learned in Vietnam, Merletti states:

“I had to learn how to evaluate the intelligence and turn that into something I can use on the ground. I learned about the uncertainties of war, that courage changes the face of everything, and that you have to be prepared. We are a product of our training and experience.”

Merletti then continued by discussing his time in the U.S. Secret service, which started with investigating counterfeit money and working undercover in organized crime groups. It is to this experience with which he credits the development of excellent instincts which helped him later on in his career. Following John Hinckley’s attempted assassination of Ronald Reagan, Merletti quickly moved up the ranks from counter assault team, then the Presidential Protective Detail.

Fast forwarding to Manila, Philippines, with President Clinton, Merletti reflected on a moment where one decision to re-route the president’s detail had lasting effects on everyone involved. The president was already late and rushing off to an important meeting *“when [Merletti] got a brief message that the Philippines intelligence officials just heard a radio transmission on a frequency that they hadn’t heard or used in months. They heard the phrase “the wedding is across the bridge” said in Filipino over the radio.”*

Merletti explained that he thought he may have once heard the word “wedding” used to mean assassination, and he knew the presidential motorcade had to cross a bridge. *“I quickly had to decide if this was actionable intelligence or if this was meaningless. All my training prepared me for this very moment. I had that gut feeling that something was wrong.”* The reroute of the motorcade delayed the president an additional 15 minutes late and he was not happy. To make sure Merletti hadn’t cry wolf, field agents checked under the bride, and sure enough,

there was a bomb there. Merletti reflects: *“Realizing and responding to actionable intelligence had worked!”*

The entire U.S. Intelligence community dove into this investigation, and upon briefing out what they had found asked *“How much do you know about a guy named Osama bin Laden?”*

In conclusion, Merletti states:

“We live in a changing world. We must prepare the changing world, we must recruit the brightest of the bright...I believe we must hold on to unchanging principles. The past is unchanging source of guidance for how we need to act. The paradigm has shifted, but principles remain the same. Advances in technology and unfolding world events have altered the way we live and work, but we can't allow that to change our fundamental values and basic principles.”

A Wicked Approach to Intelligence

Panelist: Liam Fahey, Patricia Seeman, Dr. Linton Wells

Liam Fahey, Patricia Seeman, and Dr. Linton Wells entered into an open discussion regarding “Wicked” approaches to tackling intelligence issues. This included provoking questions about unique and intriguing topic of understand, dealing with, and mitigating “Wicked” problems.

The panel classified 4 types of intelligence problems

- ❖ Structured
- ❖ Semi-Structured
- ❖ Ill-Structures
- ❖ Wicked

What are these “Wicked” problems, which demand many recourses and attention?

- ❖ Limited access to needed resources
- ❖ The intersection of multiple problems
- ❖ Involve a big problem, with many moving parts
- ❖ Have no obvious solution
- ❖ There are deeply invested interest
- ❖ Multiple stake holders
- ❖ Brought about by change

The panel then commented: “There is so much information out there but we have to make decisions very quickly.” So how do you decide to handle this?

- ❖ Determine if a wicked problem exist.
- ❖ Assess **what** the wicked problem is.
- ❖ Discern and explore nature of the wicked problem. *“The discernment of the wicked problem is fundamentally critical.”*
- ❖ Understand the organizations intelligence strategy and positon, and how you can attack the problem.

The panel then tackle the issues and questions that arise from these wicked problems, and how you handle them.

- ❖ How do you train people to be adaptive?
- ❖ Leaders and decision makers don’t want to hear the word “I don’t know”
- ❖ How to you find people with agility and a breadth of certain wide knowledge?

- It's okay to have someone that has such deep knowledge in one topic, but you need to find people that are diverse in knowledge base.
- ❖ Change is something that creates wicked problems, and wicked problems may create change. Determining and recognizing the change, analyzing the change, and thinking and acting on the analysis that you do will help address the wicked problem.
- ❖ *“Decision making is not an event, it is a capability.”* To attack a problem a group must look at the problem from several angles. And on the topic, millennials are much more comfortable with ambiguity and not knowing where the direction is heading, which can be good, but there has to be certain structures.

Regarding how to tackle these problems as a whole institution, the panel explained *“Sociology always trumps technology”* There are people at every level talking and thinking about these wicked problems. As an organization you need to find a way break through this *“clay layer”* and enable sharing of ideas at all levels.

Regarding traditional intelligence models for wicked problems, the panel said:

- ❖ Tradition models often run opposite to the wicked approach... models and strategic situation have their place, but we are talking about real ambiguity... burn the models they just aren't appropriate ...
- ❖ Have content knowledge is losing value, what is now growing in need in the ability to find your way through the mist, and how to find out what it is you need to know.
- ❖ *“Speed trumps rigor, action trumps thinking”*
- ❖ *“No lesson is ever learned until a behavior changes.”*

Conclusion

The Global Intelligence Forum and the host, Mercyhurst University, thanks all keynote speakers, panelists, attendees, and faculty and staff that helped make the 2015 forum a success.

The next Global Intelligence Forum will be held in Dungarvan, Ireland in 2017.

For more information regarding the 2015 forum or for information regarding the upcoming 2017 forum, please contact:

Michelle Henderson

mhenderson@mercyhurst.edu

(814) – 824 – 2131



MERCYHURST
UNIVERSITY