

FOSTERING INNOVATION FOR FUTURE SECURITY CHALLENGES

PREVENT • DETECT • INVESTIGATE



INTERPOL

Global Perspectives from Experts at
INTERPOL World 2017 Congress
4-6 July 2017 • SINGAPORE

The INTERPOL World Congress 2017 agenda is developed by INTERPOL and supported by the S. Rajaratnam School of International Studies (RSIS).

@ July 2017 INTERPOL

Edited by Damien D. Cheong, Muhammad Faizal Bin Abdul Rahman, Benjamin Ang and Norman Vasu
S. Rajaratnam School of International Studies

This volume is published in conjunction with INTERPOL World 2017, an event owned by INTERPOL and supported by Singapore Ministry of Home Affairs, the World Economic Forum and Singapore Exhibition & Convention Bureau.

FOSTERING INNOVATION FOR FUTURE SECURITY CHALLENGES

PREVENT • DETECT • INVESTIGATE





Jürgen Stock
INTERPOL Secretary General

Jürgen Stock was unanimously elected as Secretary General of INTERPOL in November 2014 to serve a five-year term. Previously a Vice-President of Germany's Federal Criminal Police Office (BKA), Mr Stock has more than 35 years of policing experience, with more than half of his career in a leadership role.

A proponent of good governance and strategic management, Mr Stock has a proven commitment to international policing through his participation on the boards of several European forums, the Global Initiative against Transnational Organized Crime and the Pearls in Policing think tank.

Mr Stock was a Vice-President of Germany's Federal Criminal Police Office (BKA) from 2004 to 2014, before which he held several leadership positions within law enforcement development institutions, including Head of the Institute of Law Enforcement Studies and Training of the BKA, and President of the University of Applied Police Science in Saxony-Anhalt.

Following his election to head INTERPOL, Mr Stock launched the INTERPOL 2020 initiative to review the strategy, priorities and activities of the Organization, and became the first INTERPOL Secretary General to address the United Nations Security Council.

As part of the comprehensive reform and modernization agenda of INTERPOL 2020, Mr Stock has implemented some important changes to enhance INTERPOL's policing capabilities to more effectively tackle the priority crime areas of counter-terrorism, cybercrime, and organized and emerging crime.

Prior to becoming Secretary General, Mr Stock was a Vice-President of INTERPOL's Executive Committee from 2007 to 2010 and has chaired working groups on financial and strategic development matters. Mr Stock is of German nationality and holds a PhD in Law.

MESSAGE FROM THE SECRETARY GENERAL

Law enforcement officials today are facing a challenging and demanding operating environment. As society is increasingly connected and the world becomes borderless, technologies can help law enforcement to prevent, detect and investigate more efficiently, but at the same time, they also open up possibilities for criminals. INTERPOL believes that its vision of a safer world is possible through a multi-stakeholder approach to innovation in policing.

Autonomous cars, artificial intelligence, robotics, drones and crypto-currencies in the Darkweb; these are becoming part of today's reality, which intensifies the challenge of securing our cities, major world events, borders and cyberspace.

Welcome to INTERPOL World 2017, where experts and practitioners will share how they deploy successful solutions and leverage new technologies to shape the future of policing. Learn, share and experience the technological possibilities and state-of-the-art policing solutions in action.

Jürgen Stock
INTERPOL Secretary General



Noboru Nakatani

Executive Director

INTERPOL Global Complex for Innovation

Mr Nakatani has been the Executive Director of the INTERPOL Global Complex for Innovation (IGCI) in Singapore since April 2012. The IGCI, as a research and development facility for the identification of crimes and criminals, provides innovative training and operational support for law enforcement across the globe, especially in the field of technology-enabled crime.

Mr Nakatani previously held the post of Director of Information Systems and Technology at INTERPOL's General Secretariat headquarters (2008-2011), overseeing the development of innovative IT services for the global law enforcement community. He also served as Assistant Director of INTERPOL's Financial and High Tech Crime (2007-2008) where he specialized in cybercrime and cyber security issues.

Mr Nakatani holds the rank of Commissioner at the National Police Agency (NPA) of Japan. Prior to his secondment to INTERPOL, Mr Nakatani was Special Advisor to the Commissioner General of the NPA of Japan and Director of the Transnational Organized Crime Office (2011), where he was in charge of supervising major transnational organized crime investigations as well as the formulation of strategic priorities at the national level.

Mr Nakatani was also the Senior Assistant Director for Cybercrime Division of the NPA (2004-2007). His work in this position included responsibility for policy and planning in the area of cybercrime across the nation. For example, he initiated the establishment of the Internet Hotline Center as one of the cornerstone measures to combat cybercrime, as well as represented the National Police Agency to the G8 Rome/Lyon High Tech Crime Sub-Group.

Mr Nakatani joined the NPA as a fast-track officer in April 1993, and has held various posts, such as the Executive Officer to the Minister of State and the Chairperson of the National Public Safety Commission (2001–2002).

FOREWORD

A very warm welcome to INTERPOL World 2017 in Singapore!

This year marks the second edition of INTERPOL World, once again providing a unique forum for law enforcement, government bodies, academia, international security experts and solution providers to discuss the spectrum of future security challenges and chart the way forward to combat emerging crimes.

As we face unprecedented forms of crime occurring every day in cyberspace, we need to understand the implications of this trend on law enforcement and the security community worldwide. To be truly effective in this ever-evolving and complex security landscape, preventing, detecting, and investigating crimes of the future must take a multi-stakeholder approach. At the same time, we need to foster innovation in policing to anticipate future trends and stay ahead of cyber-savvy criminals.

Under the theme of *“Fostering Innovation for Future Security Challenges”*, the Congress (a high-level dialogue) aims to focus on pressing issues in the digital age such as Darknet marketplaces, Smart City use of big data and Internet of Things (IoT), as well as migration and border management. Back to back with the Congress, a three-day trade exhibition will showcase the latest solutions for public security, which is a great opportunity to enhance collaboration and information sharing between the public and private sectors.

In our highly globalized and digitalized world, INTERPOL serves as a global platform to assist our 190 member countries in tackling a range of traditional and emerging crimes in pursuit of a safer world.

I would like to thank all of the organizations who have made this event possible, and I hope you enjoy this inside look into the world of policing and security. I wish you a fruitful and productive time at INTERPOL World 2017.

Noboru Nakatani
Executive Director
INTERPOL Global Complex for Innovation



TABLE OF CONTENTS

11

About INTERPOL

12

The INTERPOL Global Complex for Innovation (IGCI)

13

INTERPOL World 2017

14

The S. Rajaratnam School of International Studies (RSIS)

16

PwC Singapore

SMART POLICING

19

Smart Policing: A Significant Force Multiplier
Noboru Nakatani
Nur Azhar Ayob
Ng Yiwen

CYBERCRIME

40

Child Sexual Abuse Thrives in the Darkest Parts of The Internet Thorn: Digital Defenders of Children
Jim Pitkow

44

Cybercrime: Redefining the Threat Actor Landscape
Christian Karam

50

Addressing the Challenges of Cybercrime Investigation with the Help of Open Source Tools for Remote Forensics
Vitaly Kamluk

56

Outsmarting Intelligent Cyber Security Threats with Machine Learning
Nick Savvides

60

Dark Web Investigations - An Overview from the Dutch Police
Nils Andersen-Röed

64

Unmasking Criminals in the Dark Net Using Ultrasounds
Vasilios Mavroudis

66

Tackling Cybercrime - One Challenge at a Time, Collectively and Collaboratively
Maria Vello
Michael Shoukry

70

Tackling Transnational Cybercrime with Mutual Legal Assistance

Stronger Encryption or Weaker Encryption for Public Safety?
Benjamin Ang

76

Pitfalls of the "Internet-of-Things"
Rebalancing Encrypted Messaging Apps
Tan Teck Boon

FUTURE OF POLICING IN GLOBAL CITIES

84

The State of Cybersecurity in the Auto Industry
Greg Basich
Roger C. Lancot

104

The Road to Collaborative Public Safety Digital Economy or Digital Disruption?
Hong-Eng Koh

108

Drones, Counter-Drones, and AI in Policing: A Survey of Opportunities and Challenges
Arthur Holland Michel

112

The Impact of IoT on Cybersecurity and the Future of Trust in the Digital Age
Dr William H. Saito

118

As Smart Cities Transform, Safety and Security Come First
Kris Ranganath

122

Rethinking the Investigative Process
Yuval Ben-Moshe

126

The Use of Technology and Collaborative Approach to Track Terror Threats (Rio 2016 Olympics)
Valdecy Urquiza

130

A Practical Guide to Predictive Policing in Los Angeles
Commander Jorge R. Rodriguez
Mary Woodard

134

Smart CCTVs: Third Eye of Secure Cities
Robocops: Securing the Cities of Tomorrow
Muhammad Faizal Bin Abdul Rahman

IDENTITY MANAGEMENT

142

Harmonizing Global Biometric Standards? Challenges and Possibilities
Dr Benjamin J. Muller

148

Cloud Enabled Digital Identity Management
Augustine Chiew

152

Dare to Share: the Value of Public-Private Partnerships
Michael O'Connell

158

Securing the Evolving Payments World
Derek Pak

162

Law Enforcement, Migration and Border Management in an Age of Globalization.
Dr Guy Vinet

168

Secure Borders and Identity Preservation in the Digital Age
Dr Jean Salomon

174

Stopping Threats at the Border with Third Line Threat Detection
Dr Enrique Segura

180

Vision, Innovation and Cooperation: Australia's Border of the Future
Dr John William Coyne



INTERPOL

ABOUT INTERPOL

Today's crimes are increasingly complex. They are interconnected and global, and they take place on both physical and virtual levels. More than ever, there is a need for multilateral police cooperation to address the security challenges facing the world.

INTERPOL's role is to enable police in our 190 member countries to work together to fight these evolving challenges and make the world a safer place.

We provide secure access to global databases containing police information on criminals and crime, operational and forensic support, analysis services and training. Our colour-coded Notices are used to alert police worldwide to wanted people, security threats and modus operandi.

All these policing capabilities are delivered worldwide and support three global programmes against the issues that we consider to be the most pressing today: counter-terrorism, cybercrime, and organized and emerging crime.

This combined framework gives police on the ground access to real-time criminal information, so they can understand crime trends, conduct operations and, ultimately, arrest as many criminals as possible.

INTERPOL's General Secretariat is based in Lyon, France, supported by the Global Complex for Innovation in Singapore, seven regional bureaus and Special Representative offices at the African Union, the European Union and the United Nations.

Each member country runs an INTERPOL National Central Bureau, staffed by national law enforcement officials, which connects them and their frontline officers to our global network.

Action is taken within the limits of existing laws in different countries, while independence and neutrality are enshrined in our Constitution, which prohibits any activity of a political, military, religious or racial character.

THE INTERPOL GLOBAL COMPLEX FOR INNOVATION (IGCI)

The INTERPOL Global Complex for Innovation (IGCI) is a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships. Located in Singapore, the IGCI complements its General Secretariat in Lyon, France, and enhances the Organization's presence in Asia. It is housed in a state-of-the art building in Singapore conforming to the highest environmental standards.

Crime threats are changing

Police worldwide are facing an increasingly challenging operational landscape as criminals take advantage of new technologies, the ease of international travel and the anonymous world of virtual business. Criminal phenomena are becoming more aggressive and elusive, notably in the areas of cybercrime and child sexual exploitation.

The future of policing

It is crucial for police to stay one step ahead of criminals. In today's world this can only be achieved if law enforcement officials have real-time access to information beyond their own borders. The digital age has opened up immense new opportunities to police forces, providing secure communication channels and instant access to criminal data. Technological development and innovation must become our best ally.

Championing innovation

The Global Complex goes beyond the traditional reactive law enforcement model. This new centre provides proactive research into new areas and latest training techniques. The aim is to provide police around the world with both the tools and capabilities to confront the increasingly ingenious and sophisticated challenges posed by criminals.

FOSTERING INNOVATION AT INTERPOL WORLD 2017

The security landscape is evolving with the advancement of technologies. Criminals are taking advantage of technology, ease of international travel and the anonymous world of virtual business to disrupt public security and commercial stability.

Yet, technology alone cannot be the only solution to counter technological risks and threats. A strategic response has to be taken into account to fight transnational organized crime.

A conscientious effort from law enforcement agencies, businesses and citizens, is necessary to protect ourselves, our assets and our property.

Prevent. Detect. Investigate.

It is for this very reason that INTERPOL has taken the lead to organize specific security-related events that combine both congress and exhibition.

INTERPOL World was launched in 2015 as a 3-day exhibition and congress platform for interactions and exchanges between the actors confronted with security challenges and the actors developing innovative solutions for such challenges.

INTERPOL World Congress: 4-6 July 2017

INTERPOL World Exhibition: 5-7 July 2017



THE S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES (RSIS)

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous school within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific.

Mission

- Provide a rigorous professional graduate education with a strong practical emphasis
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy
- Foster a global network of like-minded professional schools

Graduate Programmes

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science degree programmes in Strategic Studies, International Relations, Asian Studies, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from more than 60 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS. A select Doctor of Philosophy programme caters to advanced students who are supervised by senior faculty members with matching interests.

Research

Research takes place within RSIS' five centres:

- **Institute of Defence and Strategic Studies (IDSS)**
- **International Centre for Political Violence and Terrorism Research (ICPVTR)**
- **Centre of Excellence for National Security (CENS)**
- **Centre for Non-Traditional Security Studies (NTS)**
- **Centre for Multilateralism Studies (CMS)**

Research is also conducted in the National Security Studies Programme (NSSP), and the Studies in Inter-Religious Relations in Plural Societies (SRP) Programme. In general, research at RSIS focuses on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.



PWC SINGAPORE

Creating value for our clients, our people and the communities we live and work in is at the heart of PwC. Our purpose binds us together – to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services.

PwC has always played a key role supporting business, the economy and therefore our broad communities and societies. Whether it is the capitals markets, tax systems or the broader economy, PwC helps them function and develop.

Our highly qualified, experienced professionals listen to different points of view to help organizations solve their business issues and identify and maximise the opportunities they seek. Our industry specialization allows us to help co-create solutions with our clients for their sector of interest.

Being a leading and responsible Professional Services firm involves actively contributing to our community and protecting our environment. Through our Corporate Responsibility efforts in FY16, 1,638 volunteers (61% of the Singapore firm) have contributed 516 man-days on skills-based volunteering and 1,232 man-days on other volunteering initiatives.

In recent years, PwC Singapore has been awarded with several awards including:

- **Best Practice Award – Biennial Singapore Accountancy Awards 2016 (for two consecutive awards)**
- **Graduate Employer of the Year – Singapore's 100 Leading Graduate Employers Award 2016 (for six consecutive years)**
- **Best in Audit Services – CFO Innovation Awards 2015**
- **Best Tax Advisory – HFM Awards Asia 2015**

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Find out more about PwC Singapore at www.pwc.com/sg



SMART POLICING
A Significant Force Multiplier



Noboru Nakatani

Executive Director

INTERPOL Global Complex for Innovation

Mr Nakatani has been the Executive Director of the INTERPOL Global Complex for Innovation (IGCI) in Singapore since April 2012. The IGCI, as a research and development facility for the identification of crimes and criminals, provides innovative training and operational support for law enforcement across the globe, especially in the field of technology-enabled crime.

Mr Nakatani previously held the post of Director of Information Systems and Technology at INTERPOL's General Secretariat headquarters (2008-2011), overseeing the development of innovative IT services for the global law enforcement community. He also served as Assistant Director of INTERPOL's Financial and High Tech Crime (2007-2008) where he specialized in cybercrime and cyber security issues.

Mr Nakatani holds the rank of Commissioner at the National Police Agency (NPA) of Japan. Prior to his secondment to INTERPOL, Mr Nakatani was Special Advisor to the Commissioner General of the NPA of Japan and Director of the Transnational Organized Crime Office (2011), where he was in charge of supervising major transnational organized crime investigations as well as the formulation of strategic priorities at the national level.

Mr Nakatani was also the Senior Assistant Director for Cybercrime Division of the NPA (2004-2007). His work in this position included responsibility for policy and planning in the area of cybercrime across the nation. For example, he initiated the establishment of the Internet Hotline Center as one of the cornerstone measures to combat cybercrime, as well as represented the National Police Agency to the G8 Rome/Lyon High Tech Crime Sub-Group.

Mr Nakatani joined the NPA as a fast-track officer in April 1993, and has held various posts, such as the Executive Officer to the Minister of State and the Chairperson of the National Public Safety Commission (2001–2002).

**Nur Azhar Ayob**

Strategic Planning Coordinator
Office of the Executive Director
INTERPOL Global Complex for Innovation

Nur Azhar Ayob is the Coordinator in the Office of the Executive Director in the INTERPOL Global Complex for Innovation (IGCI) in Singapore since August 2015. The IGCI provides innovative training and operational support for law enforcement across the globe, especially in the field of technology-enabled crime. Nur Azhar assists the Executive Director in developing the IGCI into a research and development facility for the identification of crimes and criminals, including the development of its Innovation Centre. He also co-created the INTERPOL Global Strategy to combat Cybercrime. He serves as the IGCI's focal point facilitating engagement with Singapore government agencies. Nur Azhar leads the content development for INTERPOL World Congress 2017.

Nur Azhar was previously the Vice-Chairman of the IGCI Operational Expert Group on Cybercrime (2013-2015), overseeing the development of the IGCI's specialised capabilities to combat cybercrime. He also represented Singapore at the IGCI Working Group (2011-2015), which advised the INTERPOL General Secretariat during the development phase of the IGCI. The IGCI Working Group report its findings to the INTERPOL General Assembly.

Prior to his secondment to INTERPOL, Nur Azhar was a Senior Assistant Director in the Capability Development and International Partnerships division of the Singapore Ministry of Home Affairs. He was involved in formulating strategic priorities, engagements and developing strategic capabilities to combat emerging transnational crimes at the national and regional level (ASEAN). He was also a member of the Safety and Security Industry Programme Office, collaborating with the Singapore Economic Development Board on Whole-of-Government developmental projects, including the National Cybersecurity R&D Programme.

With more than 13 years of police experience, Nur Azhar is a Deputy Superintendent of Police in the Singapore Police Force (SPF). He has experience in strategic planning, investigations, police operations, crisis management and technology development at the regional and national level. He also provided principal staff support to former INTERPOL President and SPF Commissioner, Mr KHOO Boon Hui during his INTERPOL presidency.

Nur Azhar Ayob obtained his Bachelor of Social Science (Hons) in Information & Communications Management from the National University of Singapore and his Master in Science (Strategic Studies) from the S. Rajaratnam School of International Studies in the Nanyang Technological University (Singapore).

SMART POLICING

A Significant Force Multiplier

*Co-authored by
Noboru Nakatani
Nur Azhar Ayob
Ng Yiwen*

1. TRADITIONAL POLICING

The traditional model of law enforcement is still largely a closed system based on nation states while the threats we face today are international and transboundary in nature. This is one of the reasons why policing does not always scale globally across national borders even when it involves cyberspace.

The main purpose of law enforcement has remained the same since centuries ago – to protect both citizens and the state. Yet at the same time, the security environment and policing challenges that law enforcement faces in its work have dramatically transformed. Crime is increasingly borderless and innovative, and there is a need for law enforcement agencies to leverage on technology to improve policing.

2. WHAT IS SMART POLICING

In today's world, the concept and tools of smart policing have become increasingly important to overcome current and emerging challenges to policing. Smart policing involves having a concept of information management that will ultimately improve police work through two central tenets – leveraging on the role of technology and expanding community engagement. It is vital that law enforcement agencies embrace and adopt innovative methods of smart policing to improve global security and effectively fight evolving crime trends. There exists a crucial role for INTERPOL to act as a global facilitator in addressing criminality in today's interconnected world by leveraging on technology.

3. NEED FOR SMART POLICING

Worldwide, law enforcement is facing an ever-changing operational climate amid a tight fiscal outlook. This is further compounded as new issues emerge in the global landscape. In our opinion, smart policing is essential

for two emerging issues: cybercrime and attacks on high-density cities. With the right implementation strategy, smart policing can have a significant force multiplier effect on how police work is conducted.

A. Emerging Issue: Cybercrime and cybersecurity

The Internet of Things (IoT) revolution has the potential to be transformational and at the same time, be highly disruptive. With increasing dependence on electronic devices and network connectivity in society and economies today, attacks previously thought to be of low impact and consequence have now become a concern for law enforcement. The IoT trend presents unprecedented opportunities for criminals, as seen in the widespread proliferation of cyber and cyber-enabled crimes that are quickly replacing 'traditional' crimes such as robbery and theft. Unfortunately, this trend is set to become the norm in the immediate future.

B. Emerging Issue: Attacks on high-density cities (soft targets)

The rise of global cities is a trend that proliferated greatly over the past few decades. Combined with the increasing interconnectedness of modern cities, any hard or soft attacks on high-density global cities will cause a domino effect that will have extremely devastating and far-reaching impact on the rest of the world. The most evident examples in recent years are the November 2016 terror attacks in Paris; March 2016 terror attacks in Brussels; July 2016 terror bombings in Baghdad; August 2016 terror bombings in Pakistan; May 2017 bombing in Afghanistan and recent multiple attacks in the United Kingdom (Manchester and London), amongst others.

All these events resulted in negative global consequences materializing in different ways. This includes increased volatility in global markets, as well as heightened levels of insecurity and anxiety in communities. Intense media scrutiny surface polarizing views that can widen social divisions and highlight perceived differences, with adverse effects on societal resilience.

In this context, it is now even more imperative for law enforcement agencies to learn from and prevent such attacks from recurring. INTERPOL believes smart policing is a key approach for doing so, and it is important for law enforcement to explore and exchange knowledge on the various forms of smart policing. To that end, this document elaborates on a number of recently developed innovative policing solutions and tools that have proven to yield tangible results.

4. THE SMART POLICING TOOLBOX

Advancements in technology have paved the way for smart policing and transformed how policing should be done in today's world. Law enforcement agencies should make use of social media and innovation as a key enabler of policing work. Doing so will allow law enforcement agencies to solve crimes faster and more efficiently than before.

- 4.1 Community Engagement and Social Media
- 4.2 Safe City / Analytics
- 4.3 Predictive Policing
- 4.4 Situational Awareness
- 4.5 Authentication (Biometrics)
- 4.6 Forensics
- 4.7 Robotics and Artificial Intelligence
- 4.8 General Policing Equipment

4.1 Community Engagement and Social Media

In the Internet age of the 21st century, it would be simply naïve for law enforcement agencies

to depend solely on traditional means of community engagement. While important, having a physical presence in the community is no longer sufficient to combat crime on its own. Instead, technology has made it vital for community policing efforts to take a step further by embracing social media and other technology-enabled forms of communication. This is compounded by the fact that cyber-enabled crimes have increasingly moved beyond regular cases from online fraud and sex exploitation towards facilitating terror attacks. By expanding its virtual presence online, law enforcement agencies can increase their community engagement. This then presents even more opportunities to improve policing in today's world through a myriad of ways.

Publicize initiatives, develop trust and maintain and ongoing relationship with the community

As part of its efforts to reduce crime rates, the Panama Police Force uses social media to maintain a direct and ongoing relationship with its community both online and offline. The Unidad Preventiva Comunitaria is a task force charged with “maintaining a direct and ongoing relationship with the community” in an effort to reduce crime rates. The Panama Police Force regularly updates its Facebook page to broadcast its ongoing campaigns, policies and activities to the public. Its policing strategy offers “society’s youngest and most vulnerable members, credible alternatives to the drug market, whether [in] job training or sports activities”. This method of community engagement has been successful in reaching out to younger citizens who tend to be the most vulnerable and prone to drug addiction and drug-related violence. Results have been positive with Panama’s murder rate significantly falling to 18.0 (per 100,000 inhabitants), as well as decreases in other crimes such as theft.

The importance of social media in community engagement is once again underscored by

how it has been used to bridge cultural divides between diverse populations. California's Alhambra Police Department, Arcadia Police Department and San Gabriel City Hall Police Department are examples of law enforcement agencies that have adopted social media for this purpose. As the demography of these local cities are predominantly Chinese, the police departments turned to Weibo, a popular Chinese social networking website similar to Twitter, to reach out to and engage with its large Chinese population. Weibo is used in multiple ways by the police departments to facilitate communication with the community, increase public safety awareness, encourage cooperation, and even mobilize immigrant civic engagement. This is done by disseminating information, such as updates on crime trends, city policies and events, traffic alerts and prevention tips not only in the right language, but also in a context that Chinese users can understand. This is especially since many of its Chinese residents are migrants who only speak Mandarin or other Chinese dialects.

The success of using Weibo can be seen in how the previously difficult-to-engage Chinese immigrant communities, and even Chinese citizens planning to tour the country, have started to get in touch with the Alhambra Police Department to make enquiries about law and order issues. Increased interaction with the community has improved public trust in the police as residents change their negative perceptions of the organization. This has led to better cooperation between the department and the community, a greater willingness of the community to use police services, and a better understanding of existing laws and regulations.

Though the police departments of these cities had traditionally used popular American social media channels such as Facebook and Twitter, these mediums were unable to effectively

reach out to the Chinese community. For example, the Weibo account of Alhambra Police Department garnered more than 40,000 followers over two years, as compared to its Twitter and Facebook accounts with 1,200 and 8,000 followers respectively, despite having been set up for a much longer period.

The use of popular Chinese social networking sites by the aforementioned police departments highlights the value of having a social media presence to aid community policing efforts today. This is largely because it not only prevented alienation by tapping on a platform that many Chinese residents were already using, but also because the sites provided a means for the police to interact and engage the community. At the same time, it also highlights the need for police departments to adopt flexibility, adaptability and innovation when reaching out to communities and tailoring efforts to their needs.

Provide credible information in real time

Social media allows for law enforcement agencies to be the direct source of news to the public, particularly during times of emergency. This is perhaps most evident in the Boston marathon bombings that took place in April 2013, which saw the Boston Police Department (BPD) bypassing traditional media outlets and immediately turning to social media to keep the public informed. Twitter was used to keep the public updated on the situation as it unfolded, the status of the investigation and steps the police were taking to manage the crisis. By communicating directly with the public, the BPD minimized the spread of misinformation as it ensured that only accurate and complete information was disseminated to the public through social media. In doing so, it also demonstrated transparency in public communication and kept the public calm. As a result, public trust in the BPD increased; an important outcome to combat misinformation and fake news.

It must, however, be acknowledged that the BPD's success in using social media during its investigations was in large part possible due to previous trust building efforts by the department, further highlighting that there is still a need to have a physical presence in the community.

Enabling Two Way Communication

That physical presence in the community remains necessary is highlighted in the case of the New York Police Department (NYPD). While crime in New York City has fallen to its lowest in recent decades, tensions between police officers and the communities they work with still persist. In order to deal with these tensions, the NYPD introduced a culture change in their agency, transforming their policing mindset from 'warrior' to 'guardian'. This was observable in its Neighborhood Coordination Officer (NCO) program, use of social media for public engagement, and relaxing the existing 'command and control' culture.

The NCO program represented an NYPD initiative to reduce crime and repair frayed relationships between the police and communities, which had worsened in recent years. Under this program, 166 neighbourhood summits (community meetings involving the NCOs, residents, workers and visitors of the neighbourhood) were held in the five boroughs of New York. They enabled the NYPD to meet residents, strengthen relationships and attain feedback on how crime and other problems could be better dealt with. At the same time, the NCO program also required officers to spend 20 per cent of their time 'off radio'. This meant that NCOs were expected to move around their assigned neighbourhoods, engage informally with the residents and familiarize themselves with the community. These initiatives were received favorably by the public and more importantly, helped to build trust.

The program's success is reflected in the 2017

crime statistics of neighbourhoods where the NCO program was implemented. Compared to the same period in previous years, it was reported that overall crime had decreased by 6.2 per cent, shootings had fallen by 29.5 per cent, and murders reduced by 8.5%.

In addition, the NYPD also uses Twitter as a tool to engage citizens, a shift from its traditional command and control culture. The idea behind this approach was to co-opt the public to assist the NYPD in their crime-fighting efforts. However, while regarded positively, there continues to be challenges associated with the NYPD's online engagement strategy. One key example was the unintended backlash from a public engagement initiative on social media. The NYPD's twitter campaign inviting New Yorkers to post photos with NYPD officers under the hashtag #myNYPD (which aimed to highlight the close relationship between the police and community), was ironically used by individuals to criticize the department.

Crowd-sourcing information

Traditionally, law enforcement agencies rely on public tip-offs and missing person bulletins to gather information for investigations. However, smart phones and social media have drastically altered the way people communicate today. In light of this, many law enforcement agencies increasingly turn to social media platforms (such as Instagram, YouTube, Facebook, Snapchat, Telegram and Twitter) to gather intelligence.

One such example is the Gyeongnam Provincial Police Agency in Changwon City of South Korea. Over time, officers found that the conventional method of crowd-sourcing information via wanted-person advertisements was ineffective, and turned to social media as a result. A screen capture of the CCTV footage featuring the suspect was uploaded on the agency's Facebook page, along with a description of his offenses.

Following this, the post went viral almost immediately, and the police received key information that resulted in an arrest within two days.

In Georgia, the police department of Johns Creek took a step further by developing a mobile application to increase citizen engagement and enhance two-way public communication. The application, JCPD4Me not only provides information on missing people, traffic news and community events, but also links to social media platforms and other municipal services provided by the city. Most importantly, the app posts information on the city's most wanted criminals, which has greatly helped the police department in investigations. For instance, moments after the police department posted information of a wanted suspect on all social media platforms connected to JCPD4Me, the department received useful intelligence from residents that enabled them to arrest the individual within a day.

Crime Prevention

In recent years, social media has become a primary instrument for terrorist groups to recruit and spread extremist propaganda. Perhaps the most evident example is how violent extremist narratives are disseminated over popular social media websites such as Facebook, Ask.fm, YouTube, Twitter and online blogs. This has contributed to the radicalization of many young individuals from all over the world, and in some cases, inspired them to perpetrate attacks that were falsely justified in the name of Islam.

In response to this phenomenon, the UK Metropolitan Police enlisted the help of social media-savvy young Muslims as part of its counter-terrorism strategy. The vast amount of extremist content online prompted many Muslim youths in London to come up with various ideas and suggestions to help law enforcement. This includes working together with the police alongside imams, parents

and 'disengaged' peers to combat Islamic extremism by helping to prevent online radicalization of the young. By integrating the first-hand experience of young Muslims into its counter-terrorism strategy, the Metropolitan Police attempted to improve its engagement with Muslim youths, and at the same time, crowd-source critical information to counter violent extremism. Apart from a 'shift in the mindset of the Muslim community' in London, this strategy has also resulted in more tip-offs on individuals wanting to travel from London to Syria to join terrorist group Islamic State of Iraq and Syria (ISIS), as seen in the 83 tip-offs reportedly received in 2015. The Metropolitan Police's success can be attributed in part to its use of the most suitable candidates to counter violent extremism online – social media-savvy young people within the Muslim community.

These various case studies show how social media has now become an important resource for community policing that law enforcement cannot ignore. Having an online presence removes barriers to communication and provides a framework for changing the way the community perceives law enforcement. Nonetheless, it is important to understand that law enforcement must continue to have a strong physical presence within the community. This two-way approach of balancing a physical and virtual presence will then allow for community policing and engagement to be truly effective.

4.2 Safe Cities / Analytics

Modern cities have changed dramatically in recent decades: cities have grown more congested and crime has become more complex. In light of the shrinking municipal budgets and rising costs of manpower, the model of the friendly neighborhood beat policeman now seems antiquated and quaint.

'Safe Cities' are becoming a necessity in light of an increasingly complex threat

environment. In essence, 'safe cities' utilizes a network of IoT-enabled devices as tools to improve policing tasks ranging from crime fighting to dealing with emergencies and conducting surveillance. Benefits to the law enforcement community and city governance departments include a proactive, 'smarter' approach to crime and disaster management, better allocation of resources, performance indicators, faster response time and better situational awareness. In recent years, many countries have started to implement safe city initiatives, as in the case of Singapore, China and Pakistan.

Singapore Government: Safe City Test Bed

Singapore's Safe City Test Bed is perhaps one of the best examples that showcase how technological advancement can pave the way for large-scale smart policing. The Safe City Test Bed is part of the country's wider initiative to develop a Smart Nation by using advanced analytics to complement its public safety solutions. Both approaches are envisaged to improve security and service delivery in the most efficient manner.

A single precinct of the Jurong Lake District was used as a test bed for a range of urban digital experiments. The trial involved the integration of data from diverse digital sources such as mobile and Wi-Fi, as well as government data and data from social networks. More than a thousand sensors were deployed to monitor every aspect of the precinct, and the live data obtained from surveillance cameras was then integrated and applied to various policing/public safety tasks. This included crowd control, emergency response, resource coordination, effective multi-agency collaboration, sense-making, traffic and disaster management. In addition, the system also monitored anomalies online (e.g., sudden changes in behavioral/communication patterns on social media) to improve the overall analysis.

The onset of data analytics, combined with intelligent infrastructure enables public safety to be achieved without using much resources. As advanced analytics allow for better situational awareness and sense-making, senior decision makers can deploy resources in a more targeted and efficient manner. As a result, specialist police officers and accompanying support systems can be deployed for other purposes. Most importantly, by integrating real time inputs with advanced analytics that exploit big data, more meaningful insights can be produced in real time for law enforcement officers to respond quickly to threats, as opposed to relying on static standard operating procedures.

Nanjing, China

The city of Nanjing adopted LTE technology developed by Chinese company Huawei to improve public security and improve crime-fighting capabilities. Like the Singapore Safe City Test Bed, the Huawei solution enabled authorities to integrate a diverse range of information modules and communication methods across departments and regions. Officers also had their smart devices connected to private broadband networks to access live feeds from a monitored location. Law enforcement was thus able to better coordinate responses and reduce vulnerability to cyber-attacks by using the Huawei solution.

As Nanjing was the host city for the Asian Youth Games in 2013, the city government used Huawei's technology to provide better surveillance and protection of key areas. For instance, Nanjing applied the technology by connecting drone-mounted cameras to ensure that law enforcement would not be hampered by blind spots in video networks or by low-quality imagery. By adopting the safe city concept, public safety and security during the large-scale event was ultimately strengthened.

Islamabad's Safe City Project

In July 2016, Pakistan's Capital Police Force was reported to have thwarted a major terrorist attack similar to the multiple terror attacks in Mumbai in 2008. Security snap checking to identify suspicious vehicles via state-of-the-art security equipment was made possible under Islamabad's Safe City Project. Since June 2016, around 1,850 modern surveillance cameras around the capital monitor entry and exit points, roads, commercial centers and other important buildings. Additionally, smart police cars with integrated cameras connected to a command and control center monitor difficult-to-cover areas. The combination of these different cameras enabled a faster and more accurate means of identifying suspicious and dangerous vehicles, which ultimately prevented the attack from taking place.

4.3 Predictive Policing

Predictive policing is an emerging technological approach in the domain of smart policing. It refers to the application of analytical and statistical models to help identify targets for police intervention to prevent or solve crime. Tools for predictive policing have different uses. They can range from the prediction of high-risk areas for crimes to the identities of perpetrators and victims of crimes. In recent years, many law enforcement agencies have started to experiment with predictive policing. Predictive policing represents one of the latest attempts at introducing smart policing in law enforcement. It effectively leverages big data and automated data mining in many ways that the human brain is unable to replicate. There are several benefits associated with the adoption of such tools – Firstly, it paves the way for more efficient and proactive policing (rather than reactive policing), and secondly, it provides law enforcement agencies with a more structured approach to resource allocation for better strategic planning and long-term sustainability.

PredPol

PredPol is a cloud-based crime prediction software that focuses primarily on identifying locations where crimes are most likely to occur within a specific timeframe. Initially capable of only predicting crimes like burglary and car theft, PredPol's core technology has expanded to also include predictions of drug-related crime, gang-related crime, anti-social behavior and gun violence. It has been utilized by many law enforcement agencies, such as the Los Angeles Police Department, Seattle Police Department, Florida Police Department, Maryland Police Department and Kent County Police Force.

PredPol adopts a specific geographical approach in predicting crime, and does not take into account personal information or socioeconomic factors such as race and income levels. The technology customizes predictions to different areas based on a 500-by-500 foot framework, so as to ensure all areas are covered. The PredPol system works by analyzing data through a sophisticated algorithm that applies proven criminal theories to predict the top 10 to 20 spots where crime is most likely to occur in the next few hours. To do so, it leverages on a variety of factors, such as historical and recent crime data, real-time activity and weather forecasts. Once these 'hot spots' are identified, patrol officers can then visit these locations multiple times during their shift, making their presence felt in the area, thereby preventing crime from taking place. This means that for PredPol to be more effective, community-based services and positive outreach programs must already be in place.

As the model depends on the presence of police officers to prevent/solve crime, PredPol enables officers to access its predictions on the go by linking its system to the computers onboard patrol vehicles. Due to the comprehensive and usable framework developed by PredPol, law

enforcement agencies using PredPol are of the view that the program represents a paradigm shift in how officers have conventionally done policing, and is a valuable tool in helping to reduce crime. For example, in 2014 the Los Angeles Police Department's (LAPD) Foothill Division reported a 13% decrease in crime within a mere four months after adopting PredPol, a significant improvement compared to the 0.4% increase in the rest of the city where the program has yet to be implemented. The LAPD Foothill Division also saw a 20% fall in predicted crimes over a year, and even experienced a day without crime in February 2014. Similarly in 2014, the Alhambra Police Department in California had reported a 32% fall in burglary cases, as well as a 20% reduction in vehicle theft since it started using PredPol.

Moreover, the analysis provided by PredPol has helped improve community policing efforts. In using PredPol, the Alhambra Police Department was able to increase its visibility to the community as officers spend more time patrolling the high-risk crime areas.

Geographic Information Systems (GIS)

The GIS refers to a 'smart mapping' platform that enables predictive policing. Similar to the safe city concept, it allows information aggregation from various data sources. For instance, security surveillance and social media feeds can be plotted on a map to help law enforcement agencies shorten response times by quickly collating data and improving ground sensing. Additionally, the GIS technology can also be used in the areas of cyber and supply-chain security. Users of the GIS platform include the Singapore government as part of its Safe City Test Bed. It has also been tested by other law enforcement agencies such as the Santa Clara Police Department, Boston Police Department, Los Angeles Police Department, US Department of Homeland Security as well as the Royal Malaysia Police.

In the case of the Santa Clara Police Department, officers were able to respond to a public brawl, pinpoint the location of the victim, and identify the suspects within three minutes. This swift response was due to the 'smart mapping' provided by the GIS platform as well as the system's ability to detect anomalies in the social media space (many bystanders were tweeting the incident as it occurred). The information helped officers to quickly collate and make sense of what was happening on the ground. This example highlights how advanced data analytics can play an important role in improving police capabilities in terms of responding to social disturbances and maintaining public safety.

4.4 Situational Awareness

In order to make better strategic and operational decisions, it is essential for law enforcement to improve their situational awareness. Apart from the implementation of intelligent infrastructure in smart cities, other technological innovations, such as those discussed below, can be very useful. Such innovations serve as important force multipliers while lowering operational costs. More importantly, they can be used to support police missions in many fields, such as kidnapping, search and rescue operations, bomb investigations, drug interdictions, fugitive investigations, crowd control, collection of evidence, investigations on traffic accidents, tactical operations, police pursuits, emergency and disaster response, and CBRNE/HAZMAT management.

Unmanned Aerial Vehicles (UAVs)

UAVs, more commonly known as drones, is one new technology that can be used to increase situational awareness in operations. Many law enforcement agencies, such as the Federal Bureau of Investigation (FBI), San Jose Police Department, Santa Rosa Police Department and the Dutch Police Force are using drones to conduct surveillance, gather intelligence and assist police pursuits.

In 2015, the London airport police adopted drones as part of its counter-terrorism strategy. Surveillance drones are used at the four London airports to monitor external security from the air. The surveillance provided is envisaged to allow counter-terrorism officials to carry out missions seven times faster, and reduce operational costs by at least £1.2 million. Such technological innovations are immensely beneficial as it enables more ground to be covered quickly without the need to deploy more police officers. Hence, drones represent yet another aspect of the new digital movement that can help to counter current, new-age security threats in a more effective and efficient manner.

Yet at the same time, concerns over the use of drones for malicious purposes have arisen despite it being an extremely useful tool for law enforcement. This is exemplified by the 2016 incident where a small drone containing traces of radiation was found on the roof of the Japanese Prime Minister's office. As drone technology is constantly improving, the security risks associated with unauthorized drone use naturally increases. The potential weaponization of drones for carrying out attacks is a case in point. Drones can be fitted with automatic weapons, IEDs or large payloads and used offensively.

Law enforcement agencies in many countries have therefore adopted several innovative measures to manage these risks. For instance, it has become mandatory for drones in the US to be registered with the Federal Aviation Administration, as part of its approach to address safety/security concerns. Japan's Metropolitan Police Department possesses a special drone equipped with a camera and large net to capture rogue drones. Interestingly in the Netherlands, the Dutch Police Force have turned to a low-tech solution to counter this high-tech problem. It recently experimented with using eagles to capture or take-down unlicensed drones in mid-flight.

Anti-drone technology has also been developed to mitigate the risks associated with drones. One such example is the HP 47 Counter UAV Jammer, which several law enforcement agencies have started using. The HP 47 Counter UAV Jammer has the ability to block drones up to 1,000 feet from sending data (including video feeds) back to its operators. It can also disable operators' remote access to the drone and trap it within an invisible fence. Once trapped, authorities can either capture the drone with a net or shoot it down with the help of snipers. This anti-drone technology was used by the Swiss authorities during the World Economic Forum, as well as the German police when former US President Barack Obama visited the country, to prevent any UAVs from getting too close to their locations.

Unmanned Underwater Vehicles (UUVs)

UUVs refer to underwater drones that can operate without a human pilot. Compared to UAVs, which are increasingly sophisticated and used by many police agencies, UUVs are still in the early phases of development. Given the potential benefits UUVs can bring to police work, this technology should be closely monitored by law enforcement agencies. UUVs can be particularly useful for operations involving body recoveries and/or underwater evidence-retrieval. More importantly, it can serve to ensure the efficiency, effectiveness and safety of law enforcement officers. In the near future, it is highly likely that countries with vast coastal areas or significant in-land water surfaces will deploy UUVs for police operations in the same way they use drones today.

Persistent Surveillance Systems

Like drones, the Persistent Surveillance Systems is a surveillance technology that uses airborne cameras to monitor the city and record data in real time. The system has been tested by the Los Angeles County Sheriff's

Department to monitor the city of Compton, and even to track fleeing suspects. By using these airborne cameras, law enforcement agencies can monitor a wider area of the city in a more cost-effective and efficient manner, as compared to using police helicopters or land surveillance cameras.

4.5 Authentication (Biometrics)

Biometric innovations are not limited to border security usage but can be adapted for other law enforcement purposes. Technological advancements have given rise to many biometric devices that allow law enforcement to identify suspects and criminals more effectively and efficiently.

Mobile Biometric Device

Like its name suggests, the Mobile Biometric Device is a handheld gadget that is used in the field to identify individuals by scanning fingerprints, irises and other biometric information. The information is sent to a remote DNA database for processing, and the results are transmitted to the investigator within a short period of time. Evidence technicians can use the device to scan a latent fingerprint and electronically transmit the print to a fingerprint database, which will then provide potential matches. The Mobile Biometric Device is used by the Stockton Police Department to process fingerprints at crime scenes.

The use of such a device is expected to improve police investigations as it shortens the time taken to process fingerprints. The Mobile Biometric Device has the ability to provide matches with an average response time of 10 minutes, thereby allowing investigators in the field to begin their work almost immediately. This is a stark contrast to traditional processing methods where investigators would often have to wait for days/weeks for the results. Additionally, the Stockton Police Department has reported that the device is particularly

useful in identifying suspects in cases involving commercial crimes, residential crimes and automobile theft.

Rather than replacing the traditional method of processing evidence, the Mobile Biometric Device should be used to complement existing methods. This is because crime investigations benefit when more information on a crime scene is available, and the device can potentially provide leads or identify persons of interest to approach when there are no witnesses.

RapidHIT DNA Testing Machine

The RapidHIT DNA Testing Machine is a portable device that can help investigators identify criminals and victims quickly. This is done by matching swabs taken from a crime scene against a national DNA database. The device can process DNA samples from sources such as teeth, sweatbands, cigarette butts and even clothing, and does not require any specialist knowledge to operate. The whole process takes about two hours, which is considerably shorter than using traditional DNA analysis methods. Many law enforcement agencies are currently using the RapidHIT DNA testing machine. They include: the Arizona Police Department, Tucson Police Department, Pima County Sheriff's Department, Alameda County Sheriff's Department, Richland County Sheriff's Department, Palm Bay Police Department, US Department of Justice, Department of Homeland Security as well as the crime lab in Orange County, California. The RapidHIT machine has been used in investigations involving burglaries, violent crimes, immigration offences, tracking suspects and human trafficking.

This technology gives law enforcement an edge by generating investigative leads, identifying potential suspects and providing evidence quickly. For example, the current system for most California law enforcement agencies

involves shipping DNA samples to a state lab where DNA analysis can take up to weeks or months. The lab is often overwhelmed and cannot process the samples expeditiously, thereby delaying overall investigations.

Facial Recognition Software

Facial recognition software is an advanced forensics biometric technology that was first developed in the 1960s, but has only recently evolved to become accurate enough for widespread use. It generally works by extracting key facial identifiers from a still photo or video image of an individual, and then comparing these identifiers to biometric profiles in a criminal database. For instance, the software is able to determine if an individual is wanted within seconds simply by comparing his/her eye size or shape of the nose bridge against information from an INTERPOL database. An added advantage is that an officer can also access this information through a mobile device.

Facial recognition software is commonly used by law enforcement agencies to identify individuals in crowded areas. It is also particularly useful for locating suspects on the run, border security, conducting missing persons searches and pre/post-attack surveillance.

The Leicestershire Police for example, used NEC's facial recognition software 'NeoFace' to enhance public safety and security during 'Download', a large-scale outdoor music festival that saw almost 100,000 attendees. The digital images (including low-resolution ones) captured by the software, were matched against a database of criminals in Europe who specifically targeted music festivals.

The San Diego Police Department's fugitive task force also relies on facial recognition software to search for wanted criminals in high-profile violent crime cases. In addition,

the Honolulu Police Department uses the MorphoFace Investigate system developed by Morpho, to determine if a suspect is linked to a particular crime by analyzing his/her facial identifiers from an image.

Facial recognition software can be used in conjunction with spatial-temporal profiling technology to detect behavioral anomalies. The 14 international airports throughout Brazil have adopted technologies developed by NEC to enable officials to identify watch list individuals easily and alert authorities in real time, thereby enhancing the effectiveness and efficiency of customs procedures and border control.

Considering there can never be sufficient resources to deal with the widespread proliferation of crime, facial recognition software empowers law enforcement to carry out "upfront crime prevention" amid a complex and vulnerable security landscape. Other law enforcement agencies using facial recognition software include the Seattle Police Department, Boston Police Department, Federal Bureau of Investigation, US Immigration and Customs Enforcement, and the US Border Patrol.

4.6 Forensics

Forensics is critical in any investigation, be it chemical or digital analyses. Technological advancements have paved the way for law enforcement to obtain forensic information quickly and convert it into actionable intelligence.

TruNarc Handheld Narcotics Analyzer

TruNarc Handheld Narcotics Analyzer is a mobile device that can identify more than 100 substances, cutting agents and precursors within seconds. Using Raman spectroscopy, the device is able to quickly determine the composition of the stimulant, depressant, analgesic or hallucinogen. Upon identifying

the substance, the device will automatically capture the results, date and time stamp the results and provide automated reports to law enforcement officials. The device does not require samples to be taken by direct contact, and the number of different substances that TruNarc can identify is updated every three months to include new and emerging drugs in its database. Law enforcement agencies using TruNarc include the South Australian police, Yarmouth police, Gadsden Police Department as well as the Franklin County Sheriff Department.

A mobile device capable of identifying substances in near-immediate time, TruNarc is yet another innovation of smart policing that will greatly benefit law enforcement in many ways. It brings immediacy to investigations involving drug dealing and trafficking; helps law enforcement stay ahead of the constantly evolving narcotics threat; increases officer safety when dealing with harmful substances; and eliminates the possibility of any contamination of evidence. In helping to improve the efficiency and effectiveness of law enforcement in getting illegal drugs off the streets, TruNarc also contributes to improved public safety and security, as there is a high likelihood that crimes motivated by drug use and addiction, such as assaults and robberies, can be reduced.

Compared to existing methods of sending drug samples to a laboratory for analysis, TruNarc expedites this process. This, in turn, enables the police to formally charge the suspect in a shorter time. The Gadsden Police Department for instance, used TruNarc to analyze a small bag of meth within 30 minutes. In 2013, the Gadsden Police Department took three days to conclude investigations that would have taken 18 months if the samples were sent to a laboratory, which subsequently resulted in the seizure of over 700 bags of synthetic marijuana. Similarly in 2014, the Franklin County Sheriff

Department also used the device to speed up investigations, which led to the seizure of over 8.8 pounds of methamphetamine. Given the speed and accuracy in which TruNarc identifies substances, the device can benefit various law enforcement agencies such as police departments, customs and border patrol officers.

Synthetic DNA Spray

Although the introduction of synthetic DNA increases the possibility of criminals manipulating it to perpetuate crime, it also offers law enforcement additional solutions for crime-fighting.

Using synthetic DNA put together by mathematical algorithms, unique lines of DNA code can be created for every individual building or home. Invisible to the naked eye, odorless and virtually impossible to be washed off, the synthetic DNA glows in a bright shade of blue under ultraviolet light. When sprayed onto a person who enters or exits a building or shop, the chemical traces left on him/her provides investigators with hard evidence to identify as well as connect the individual to a crime at a specific location. Furthermore, as the synthetic DNA solution stays on the skin for almost two months and clings to clothes, it provides investigators with the necessary forensic evidence to support ongoing investigations even after days or weeks have passed.

The main advantage of using the synthetic DNA spray is deterring crime. By placing a sign in the store/establishment warning patrons that the system is in use, potential shop-lifters may be deterred as the risk of getting caught is higher. Business and home owners who have used the system have reportedly experienced a decline in break-ins and theft.

Companies producing this technology are DNA Security Solutions and Selecta DNA. The

technology is currently in use in more than 30 countries, including Australia, New Zealand, United States and the Netherlands.

Cellebrite Universal Forensic Extraction Device (UFED) Software

Given that computers, smartphones and tablets have become part and parcel of daily life today, gaining lawful access to the content in these devices can significantly impact the outcome of investigations. The Cellebrite UFED Link analysis is an example of a digital forensics software with the ability to distill a wealth of mobile data into meaningful formats for law enforcement, removing the need for officers to engage in tedious manual analysis.

To retrieve data from mobile devices, investigators simply plug the device into a computer installed with Cellebrite software. The software enables investigators to access the data in mobile devices. It would then only take two to three minutes for the software to search through the device for call records, GPS locations, and application data. The software can even recover deleted data. The software also has a timeline feature, which displays the interactions between the user and his/her acquaintances in a single diagram. This data is particularly helpful in speeding up investigations by revealing motives and establishing relevant connections between suspects and victims.

Digital forensics is primarily used to obtain critical evidence needed to convict criminals such as sexual predators, murderers and terrorists. For instance, the Boulder Police Department used the Cellebrite software to access data in the mobile phones of drug-overdose victims to uncover the identities of drug dealers. The Connecticut Police Department used Cellebrite technology to recover a series of incriminating text messages that were deleted from the mobile phones of murder victims, which subsequently resulted in the arrest of the murderer.

Wynyard Digital Evidence Investigator

With the prevalence of digital evidence today, law enforcement now have to analyze vast amounts of complex data. The Wynyard Group's Digital Evidence Investigator, a criminal analytics technology that processes, locates and analyzes the electronic evidence contained within confiscated digital devices, is designed to help law enforcement meet this challenge. The technology, developed in association with the New Zealand Police, can benefit police agencies, customs and border control, fusion centres, and homeland security.

New Zealand Police have used the Wynyard Digital Evidence Investigator to deal with a myriad of crimes such as drug-dealing, child sex offences and even financial crime. The speed of analysis provided by this technology is exemplified in how the New Zealand Police used it to extract and uncover incriminating evidence from a USB stick carried by a suspected pedophile. The information obtained via this tool eventually led to the arrest of the suspect, but more importantly, was used to locate the victims.

Project Spotlight by Thorn

The Internet has, unfortunately, become an enabler of human trafficking, and in particular, child trafficking. In the US alone, the number of human trafficking cases has increased exponentially over the years. Unfortunately, the sheer amount of data, combined with the use of the Dark Web by criminals to mask their activities, makes it very difficult for law enforcement to deal with such cases expeditiously.

Spotlight is a web-based application developed by Thorn to address this challenge, but also transform the massive amounts of data into an asset for law enforcement. Thorn is a company that focuses on defending children against child sex trafficking, dark web child abuse and exploitation, as well as operating as a social

platform for cyber safety. Spotlight leverages on digital footprints to better analyze and track data, which can ultimately lead to the discovery of the traffickers and their victims. It is a neural net that gets more intelligent and efficient each time the software is used.

More than 4,000 officers from 780 law enforcement agencies all across the US have adopted Spotlight in their work. The Federal Police of Honolulu for instance, regards Spotlight as “a force multiplier at every stage of the operation” and “allows us to conduct faster, more precise investigations that will remove criminals from the street and most importantly, recover victims”.

In 2016, 6,325 victims, 1,980 children and 2,186 traffickers were identified through Spotlight. By reducing investigation time by at least 60%, Spotlight enables law enforcement officers to better manage their caseload. Spotlight makes tracking down traffickers and their victims much faster and easier for law enforcement, and shows how the Internet can in fact become a disabler of human trafficking.

4.7 Robotics and Artificial Intelligence

In light of an increasingly complex threat environment, smart policing has become essential in protecting citizens in modern cities. Technological advancements have paved the way for robotics and artificial intelligence to support and improve smart policing work.

Telerob Explosive Ordnance Disposal and Observation Robot (tEODor)

tEODor is primarily a state-of-the-art bomb response robot that can be used for several tasks. It has the dexterity to handle an egg, but also has enough power to crush a door lock. It can lift 100kg with ease, has four high-resolution cameras and can be equipped with weapons such as shotguns or water cannons. Given these specifications, tEODor is not only

suitable for dealing with bomb threats, but also for surveillance and attack purposes.

tEODor has the ability to detect, disarm and dispose of bombs and car bombs – all while gathering on-site intelligence for police officers. For instance, the Northern Territories bomb squad in Australia used tEODor to access and remove a homemade pipe bomb that was found near a residential area. tEODor’s versatility was underscored when Queensland Police used it to carry out thorough vehicle searches in Brisbane ahead of the G20 summit. As such, the tEODor brings about significant benefits to law enforcement, particularly in its ability to safely neutralize bomb threats and improve situational awareness.

iRobot Packbot

Like tEODor, the iRobot Packbot is another hi-tech solution for law enforcement to enhance public security and officer safety. The Packbot is a remote-controlled tactical mobile robot small enough to reach under large vehicles. It’s other features include: a robotic arm with an increased reach of over 6 feet to grip or manipulate objects; bright lights to illuminate a vehicle’s interior; the ability to travel up to 5.8 miles per hour, climb stairs, maneuver itself over tricky terrain and be submerged in up to 3 feet of water; four different cameras that allow users to monitor a situation and control the robot through a laptop screen; a ‘disruptor’ feature that shoots rubber rounds or water at an object; and a 4.Hz mesh video kit that can establish and relay communication in radio-challenged environments.

In light of these features, the Packbot is used for similar purposes to tEODor – identification and disposal of potentially dangerous objects; obtain situational awareness in potentially dangerous environments; and communicate with individuals where regular communication channels are malfunctioning (such as disaster areas).

The Packbot has been used by law enforcement on several occasions. During the 2014 FIFA World Cup event, the Federal Police and other local police forces throughout Brazil used the Packbot to provide public safety support. It was used to support security screening by examining suspicious packages. This kept operators safe and allowed the police to deploy manpower elsewhere. The Packbot also helped support the BPD's manhunt and arrest of the Boston Marathon bombing suspects. Before attempting to arrest the suspects, the vehicles driven by the suspects were thoroughly inspected by the Packbot to ensure it safe for BPD officers to approach. The versatility of the Packbot therefore makes it a useful tool for ensuring safety and security.

Connected / Autonomous Vehicles

As cars become even more connected and autonomous technology improves, the cybersecurity risks also increase. Adversaries may exploit system vulnerabilities in autonomous vehicles to adversely affect public safety and security. For instance, one possible scenario involves hackers carrying out ransomware attacks by installing malware onto a vehicle's operating system to disable the driving functions of the car. This can be done easily through the vehicle's unprotected Internet connection, Bluetooth or infotainment system. Hackers can also make use of this vulnerability to take full control of the vehicle. In 2015, ethical hackers uncovered a major security flaw in autonomous vehicles using a simple computer hack.

Another plausible scenario is the weaponization of autonomous vehicles to conduct terror attacks. Unlike the suicide attack carried out in Nice where the perpetrator drove a cargo truck into a crowd in July 2016, hacked autonomous vehicles increases the risks of a similar incident recurring.

Given these scenarios, automotive security

companies such as ARGUS Cyber Security have developed solutions to address these challenges. ARGUS Cyber Security has developed an integrated solution to enhance the security capabilities of connected vehicles against car hacking. Their technology works mainly by detecting and preventing advanced cyberattacks from penetrating vulnerable connections and reinforcing the security of critical functions of the vehicle. This creates a critical defensive layer against hackers, while continuing to support the secure and private use of connected automotive technologies. Companies like ARGUS Cyber Security are valuable partners to law enforcement, as they can help provide technological solutions to emerging security challenges related to autonomous vehicles.

4.8 General Policing Equipment

General policing equipment have also been improved through emerging technologies, which translate into greater operational advantages.

Starchase GPS Tagging System

Police pursuits usually involve high-speed chases, which often put the lives of bystanders, drivers, police officers and suspects at risk. In the US alone, it has been reported that more than 55,000 injuries occur each year as a result of pursuit-related crashes.

Starchase is a 'pursuit management technology' that aims to reduce the need for dangerous, high-speed car chases. The Starchase GPS tagging system works when officers activate the in-car launcher that shoots a bullet-like GPS tracking device that attaches itself to the target vehicle. The GPS trackers are tipped with industrial-strength adhesive to ensure that they do not detach from the moving vehicle. Once attached, the GPS movements are plotted on a digital map for both officers and dispatchers, providing officers with more time to make informed

decisions in relation to how best to pursue the fleeing suspect. The Milwaukee Police Department reported 52% less pursuits, 77% less pursuit-related crashes and 47% less injuries and deaths resulting from high-speed pursuits among its officers after using the Starchase GPS tagging system.

The idea behind the Starchase device is that criminals will eventually slow down when they think they are not being chased, making it much easier and safer for police officers to continue the pursuit. The GPS tag can relay information back to dispatch for several days, and officers can choose to deactivate it at any time. Furthermore, all the tracking data can be downloaded and used as evidence in a court of law, making it much easier to prosecute criminals. As the tracker is visible, using the Starchase GPS tag eliminates the need to attain a warrant, unlike other GPS units that are usually hidden underneath cars. Law enforcement agencies using this technology are the Milwaukee Police Department, St. Petersburg Police Department, Austin Police Department, Duluth Police Department, Delta Police, Arizona Highway Patrol, and the Iowa Highway Patrol.

The Starchase device is a useful tool for investigations. For instance, the St. Petersburg Police Department's Auto Theft Unit frequently uses the device to track vehicles stolen by teenagers. Similarly, law enforcement officials in Arizona have used this device in cases involving drug or human trafficking.

5. CONCLUSION

The future of policing should encompass new technological innovations. This document has laid out a number of key examples of innovative policing solutions and tools already available to law enforcement agencies. Technological advancements today present invaluable opportunities for law enforcement to improve policing in a world with diverse

criminal challenges, largely in terms of increasing the efficiency and effectiveness in fighting crime.

Relying on traditional means will no longer suffice and will only result in law enforcement constantly lagging behind criminals. Instead, it is now time for law enforcement to start embracing and incorporating the concept of smart policing in order to improve public safety and security for its citizens.



CYBERCRIME

Shedding light on the “Dark side”– Cyberspace and the future of security. Managing cyber threats to society from the “hidden” internet.

Changes in technology, society and in the law make new crimes possible. Attitudes are changing too. The implications of these shifts are complex. This is clearly seen in the way law enforcement and businesses have had to adapt to deal with risks and opportunities presented by an ever-changing digital environment.

The Internet and social media have been used by criminals to carry out recruitment, solicit illegal business, and perpetrate fraud, among others. The Darknet is a part of the Internet where individuals can interact anonymously online. The Internet and the Darknet within it have enabled an unprecedented globalization of crime, allowing criminals to carry out illegal business anonymously around the world, often undetected by the authorities. Darknet marketplaces are increasingly used to profit from proceeds of crime and procure illicit drugs, weapons and counterfeit identity documents, benefiting the perpetrators of terrorism, illicit markets, organized crime and a myriad of other transnational crimes.

As such, many security and law enforcement leaders have stated that the emergence of the Darknet as a trading platform will see investigations focus on the clandestine corner of the Internet, where criminals hide behind encryption and anonymization technology. New policing tools are needed to leverage on social media to prevent and detect crimes. The future of law enforcement must adapt to a changing policing environment and societal scrutiny.

How can law enforcement better understand the impact of the underground economy online? How can we build better capabilities to understand and solve crimes that exploit social fault lines? What are the underlying social and technological causes of cybercrime that law enforcement needs to understand, to mitigate its effect effectively? How do criminals exploit the Darknet to enhance their criminality, coordinate, recruit and spread their ideology? What risks and opportunities lie in emerging technology in cyberspace?

Managing cyber threats require addressing critical issues that law enforcement face in trying to make cyberspace safer for its users. The issues include policies, policing skills/techniques, public education and also legislation.

**Jim Pitkow**

Chair Technical Task Force
Thorn

Jim is a serial entrepreneur who specializes in translating emerging technologies into practical applications. As Chair of Thorn's Technical Task Force, he has worked with commercial partners to develop innovative solutions to fight the sexual exploitation of children including the Industry Hash Program, Project VIC and Spotlight. Jim started his career prototyping some of the first uses of the Web for NASA then as a Research Scientist at Xerox PARC. He received his Ph.D. in Computer Science from Georgia Institute of Technology.

CHILD SEXUAL ABUSE THRIVES IN THE DARKEST PARTS OF THE INTERNET

Thorn: Digital Defenders of Children

*Authored by
Jim Pitkow*

It is not every day that you are called upon directly to change the course of one individual's life in a clear, purposeful way. But when you are, it stays with you. And, when you fail, it sticks even harder.

Three years ago, our organization, Thorn, was called upon to help law enforcement identify a child whose images were being distributed in a child abuse forum operating in the Darknet. By the time investigators began the search, the girl's images had been circulating for more than two years.

Because the perpetrators operated in the Darknet, and had removed all identifying information from the images, investigators had little information to work with. Thorn was asked to assist in finding advanced facial recognition tools that could help match this little girl's face to publicly available data on the Open Web in an effort to find her quickly.

Existing technologies could not easily scan major public image databases at scale to help identify the child. We failed and her abuse continued for another year and a half. Finally, investigators were able to use other clues to find this child.

Over the 5 years of this child's abuse, nearly 1,000 images and videos of this child were distributed in the Darknet, and are now in open circulation joining the millions of other child sexual abuse images that feed the growing demand for abuse content globally.

This is a prime example of the darkest side of new innovations and illuminates the need for investment to combat abuse and exploitation as new technologies emerge.

Over a decade ago, the United States Naval

Research Laboratory created a tool-TOR-for the purpose of protecting naval communications online. Tor is a free software that enables anonymous online communication. It transmits communication through a global network of thousands of relays to protect a user's location and identity. The network it creates is often called the Darknet.

The benefits of this technology goes beyond protecting military communications to providing a secure way for vulnerable members of society (e.g., political dissidents, citizens of oppressive governments, whistleblowers) to communicate over the Internet, and avoid possible observation or retaliation. There are many good and noble purposes for this technology.

Yet, as with so many innovations, there have been unintended consequences. Political dissidents are not the only ones using internet anonymizing tools, like Tor. Such tools are also being used by criminals and exploiters, including human traffickers, weapons traffickers, drug traffickers, child abusers and many others. Today, the anonymous Darknet has become an open market for the trading of the most extreme child sexual abuse content.

Because the Darknet is not indexed and sites are unreliable, it is difficult to measure the exact size of the child sexual abuse material marketplace, but a recent study by Daniel Moore and Thomas Rid, both of King's College London, have attempted to do so. It is estimated that while child sexual abuse sites account for between two to three percent of the sites on the Darknet, they account for around 80% of Darknet traffic. We know that there are hundreds of sites (not all active at any given time) that may host child abuse content, and there are hundreds of thousands of images

and videos of child abuse being published in this environment each year.

The Darknet poses a multitude of challenges for investigation and identification. TOR is not indexed and therefore not searchable. It is difficult to identify new sites that are used to discuss and distribute child sexual abuse material. New sites come up and sites go down temporarily or definitively, leaving no trace of the digital footprint of abuse. Files shared on file sharing sites 'time out' - each shared file needs to be downloaded within a short period of time after it is uploaded.

Knowing 'who' is 'who' and how they are associated (admins, content-producers, clients, etc.) takes a significant amount of time to determine. Identification of new victims or a new image associated with a victim is next to impossible to keep up with.

At Thorn, we are working to address these challenges and to provide law enforcement with the tools needed to surface intelligence that leads to the quick identification of victims of child sexual abuse material, as well as the key actors that produce and promote this material in the Darknet. Our work focuses on detecting new sites, collecting data, prioritizing information, connecting disparate pieces of information to make sense of the bigger picture, integrating identification tools and improving collaboration globally.

The key to success in this work is leveraging advanced technologies that are already deployed in other fields. We're able to tap into private industry investments through our Technology Task Force, such as Microsoft's work on age progression and facial recognition through Project Oxford. In addition, we turn to government investments as well, and have looked to the research coming out of the DARPA MEMEX project to inform discovery and collection. The overarching goal is to co-opt the

best and brightest minds in IT and harness the most advanced technologies on behalf of some of the world's most vulnerable children.

Today, governments around the world spend millions of dollars on innovation focused on defense and yet the teams working on behalf of these children are often left with decades old technology at their disposal. As a non-profit organisation, we are closing that gap by building new applications via our own dedicated production teams, and connecting the dots between existing public and private investments that can make dramatic changes in this field.

In 2014, we released our first product, Spotlight, which helps law enforcement identify child sex trafficking victims sold online. Today, that product is deployed across the United States and Canada, and has helped identify more than 6,000 victims of trafficking. It has also helped cut law enforcement investigation time by more than 60%. It is transforming the way these investigations are handled - bringing the needle in the haystack to light quickly and giving investigators the information they need at their fingertips.

The work we're doing in the Darknet has a similar focus. Our tool, Solis, is currently being tested in eight countries with federal agencies that specialize in Darknet child abuse investigations.

Our goal is to never let another child linger online for years with the world watching her abuse. We will arm front line investigators with the tools they need to focus on new abuse quickly, and put at their disposal the full range of technologies to help identify and rescue victims.

Join us in this mission at www.wearethorn.org.



Christian Karam

Global Head of Cyber Threat Intelligence
UBS AG

Mr Karam is the Director and Global Head of Cyber Threat Intelligence at UBS where he oversees the bank's threat intelligence service that enables the delivery, consumption, analysis and actioning of cyber threat intelligence from various sources to provide the bank with risk awareness and the operations teams with valuable intelligence to identify threat indicators, tactics, techniques and procedures that inform and enable the timely mitigation and response to threats. Also in his role, Mr Karam conducts security research and excellence activities in thought leadership specifically in the area of security and cybercrime.

Prior to joining UBS, Mr Karam was the head of the cyber research laboratory and the lead cyber threat researcher at INTERPOL. Mr Karam developed the activities in the fields of global cyber threat research, future trends analysis, cyber intelligence and R&D within the INTERPOL Global Complex for Innovation (IGCI). Prior to joining INTERPOL, Mr Karam was an independent security researcher, penetration tester, and security consultant for several private sector firms.

Mr Karam's subjects of interest and expertise are threat intelligence, threat research, cybercrime, darknets and underground economy. Mr Karam researches also blockchain technology and cryptocurrencies for potential future threats and abuse around money laundering and criminal activities.

Mr Karam is a member of the INTERPOL Global Cybercrime Experts Group, a member of the BlackHat Review Board and an accomplished public speaker covering highly rated security conferences, governmental events and think tank forums.

CYBERCRIME: REDEFINING THE THREAT ACTOR LANDSCAPE

*Authored by
Christian Karam*

Innovation is the key component that has allowed crime to evolve throughout the ages. Criminals are great innovators at heart and have always developed disruptive technologies, as well as pioneered the discovery of unconventional ways to use new and emerging technologies that can be leveraged for their own gain. Today's criminals understand the importance of changing their behavior and modus operandi, while embracing the important technological advancements and the high dependency on the digitization of our world to mark another leap in crime history. Drug dealers, weapons traffickers, money launderers, fraudsters and cybercriminals have transformed and bolstered their operations by shifting their ways and their core focus on digital elements that allow them to minimize their efforts but maximize their profits. In this short paper, we will review specifically the evolution of the cybercrime threat actor quadrant as well as organized crime's evolved capabilities.

The Threat Actor Quadrant pre-2013



Threat Actor Quadrant prior to 2013 – Fig.1

The threat actor quadrant (which excludes insider threat) is a high level representation of threat actor capabilities mapped by skill level versus quality of intelligence that the threat actor may have access to. Prior to 2013, threat actors were categorized in 4 quadrants:

Low Skill; Low Quality Intelligence (LS;LQI)

- In this category, threat actors are politically or ideologically motivated. Typical examples of threat actors in this area are tied to hacktivism and terrorism who have been known to use tools that are automated and require little skill or knowledge to operate them. Their attack tactics would usually revolve around defacement of public websites and Distributed Denial of Service (DDoS) attacks against entities in order to protest or to disrupt the availability of services causing significant financial losses to the organization. It is estimated that the cost of a high bandwidth DDoS attack against large companies could go up to USD 100,000 per hour.

High Skill; Low Quality Intelligence (HS;LQI)

- Lone wolf cybercriminals are extremely skilled individuals that may cause significant damage to their targets, but have little understanding of how to monetize their attacks and to maximize profit given the lack of quality intelligence enabling high impact attacks against their victims. Their goal is to raise notoriety and reputation in cybercriminal circles.

Low Skill; High Quality Intelligence (LS;HQI)

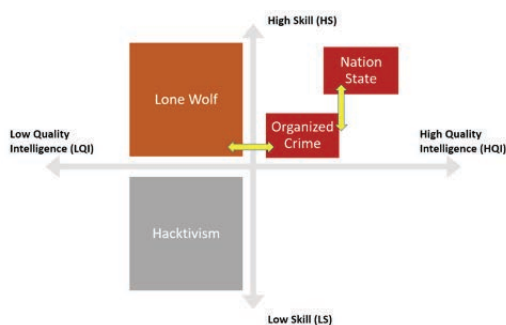
- Organized crime sees cybercrime as a business problem that needs to be further refined. Organized criminals are financially

motivated and will typically buy weaponized and finished malware from developers to use in a carefully built and efficiently run campaign. Their focus will be always on refining the business plan for a higher return on their investment. Prior to 2013, organized crime groups were slowly maturing their capabilities and skills. What highly characterizes organized crime is their access to high quality intelligence that allows them to identify important targets and victims. Data theft, extortion, fraud and carding are some of the numerous modus operandi used by the organized crime groups during that period.

High Skill; High Quality Intelligence (HS;HQI)

- The cherry on the top. Nation states have it all, skill, resources and high quality intelligence. Nation states are the most advanced threat actors on the quadrant and have matured their operations over the past years, mainly focusing on cyberespionage campaigns against political adversaries.

The Threat Actor Quadrant post-2013



Threat Actor Quadrant post 2013 – Fig.2

Post 2013 (Post Snowden), more attention and research was focused on nation states capabilities. This led to a series of incremental

evolutions in the threat actor quadrant – most notably in the shift of organized crime in the HS;HQI – High Skill; High Quality Intelligence quadrant.

Low Skill; Low Quality Intelligence (LS;LQI)

No change from a threat actor focus but the commoditization of cybercrime tools allow hacktivists and terrorists to have a larger and more effective arsenal of tools especially in the DDoS space. First seen in 2016, the Mirai botnet is seen as a high impact tool that can be rented as a service to inflict significant damage against target victims. These are still considered as the least worrying type of threat actors due to the lack of coordination and the low quality intelligence, but it is important not to underestimate the impact that such attacks could have against organizations.

High Skill; Low Quality Intelligence (HS;LQI)

Lone wolf cybercriminals were the equivalent of freelancers and now have found a permanent or contractual setting with organized crime groups to bolster their capabilities and use their skills in much more elaborate operations that aim to expand threat actor capabilities and impact in the 5th domain.

High Skill; High Quality Intelligence (HS;HQI)

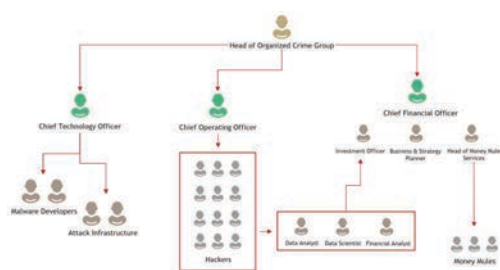
As stated previously, organized crime went through important changes in tactics, operations and structure.

- 1) Hiring lone wolf cybercriminals and hackers was done to expand and mature the skill level needed to run operations internally as seen in Fig.2.
- 2) Studying nation states' tools and capabilities while learning from their operational security planning, structure and tactics to inspire an uplift in the organized crime groups' capabilities. Organized crime did not try to completely

replicate the nation states' model, but rather kept evolving key elements to its already existing criminal enterprise model (Fig.3).

It is important to note that organized crime still continues to purchase finished malware. Due to the commoditization of cybercrime tools, organized crime continues to invest in such weaponry while delivering attacks in a more targeted, structured and tactical approach with a clearer goal and motive to its victims.

The criminal enterprise model



Criminal enterprise model in an organized crime group – Fig.3

In the criminal enterprise model, the head of the organized crime group operates similarly to a chief executive officer. This role is supported by 3 officers. A chief technology officer that keeps an oversight on the malware development operations (which organized crime did not focus on prior to 2013) and the expansion/maintenance of the attack infrastructure. Malware development is key to make sure that the payloads are always updated for a higher and more successful infection rate. The attack infrastructure is very important to maintain and to grow in order to continue generating new attack surfaces against the target victims.

The chief operating officer is in charge of running the active day to day operations of the targeted campaigns that the organized crime group is running against selected victims. Once targets are compromised, the stolen data will be sent laterally to the CFO function where a group of data analysts, scientists and financial analysts will examine the data and push recommendations to the CFO and the business planning unit to refocus efforts on a new target that may be of interest or to directly act on financial intelligence that would lead to gain and profit by investing in markets. Information has become for many years now currency 2.0.

No organized crime group would exist without a money mule and cash out unit. This is a classic unit inherited from the traditional crime models. That being said, money mule operations have seen a few updates from a modus operandi perspective to incorporate bitcoin (the currency of choice for the past few years in the cybercrime circles) as a main method of payment and cash out.

By maturing this structure, organized crime is able to bind smart, agile and effective business strategies to malware campaigns which allows them to maximize their profits. Ransomware is a great case example since it is currently a large global pandemic that was able to exponentially grow its damages and raise considerable profits for cybercriminals due to the ongoing innovation around its business models that has proven to be very successful against its victims.

High Skill; High Quality Intelligence (HS;HQI)

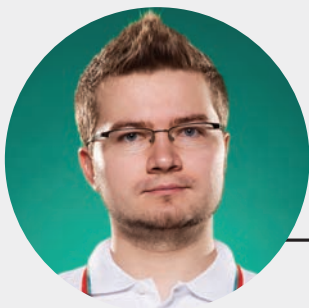
- Nation states have seen their operations closely monitored by security firms over the past 4 years. This has led nation states to often mimic organized crime or to open source their tools and share them with organized crime groups in order to blur the attribution process in campaigns that are

being tracked globally against them. It is not uncommon to see nation states hiring and recruiting organized crime to operate as a proxy in certain targeted operations. Nation states continue to grow in influence and to be the most lethal threat actor group in the quadrant.

collaborative approach from all industries and authorities is needed to ensure that we are able to counter such fast evolving and dangerous threats.

In 2006, security researchers were always on the lookout for new malware that had a serious impact on computer systems. The goal was to always provide an antidote to those anomalies and to stop it from spreading further. This problem was defined back then as trying to find the needle in the haystack. A swift and coordinated response from the industry was always needed to ensure that safety and security online was achievable. In 2010, cybercrime operations started using more complex malware and more ingenious business models, therefore researchers had to follow different trails and several different elements of the digital investigation to identify the full threat picture. This was described as trying to find the needle hidden in many haystacks. Today in 2017, with the complexity of the threat landscape and the threat actors, it is becoming even more difficult to attribute and to understand the motives, intent, and real capabilities of the adversaries and cybercriminals. If one should follow the previous analogies, the problem would be described as finding needles in a stack of needles. Advanced threat actors are mimicking each other relentlessly and are interchangeably using their tools with common interest of killing attribution process as much as possible.

It is imperative for law enforcement and for the security community to go beyond blocking the attack to identifying and putting the attackers behind bars. It is only then by stopping the fingers operating behind the keyboard, that a real impact can be achieved in securing cyberspace, and that's why a

**Vitaly Kamluk**

Director, Global Research & Analysis
Team APAC
Kaspersky Lab

Vitaly joined Kaspersky Lab in 2005 as an Infrastructure Services Developer for the Antivirus lab. In 2008, he was appointed to the position of Senior Antivirus Expert before becoming Director of the EEMEA Research Center in 2009. In 2010, Vitaly spent time working in Japan as a Chief Malware Expert, leading a group of local researchers. He specializes in threats focusing on global network infrastructures, malware reverse engineering and cybercrime investigations.

In 2014 Vitaly moved to the INTERPOL Global Complex for Innovation in Singapore to support the launch of the IGCI's Digital Forensics Laboratory and to provide high-level advice on site. In 2015, Vitaly was appointed to the position of Director of Kaspersky Lab's Global Research and Analysis Team in the Asia Pacific region.

Prior to joining Kaspersky Lab, Vitaly worked as a software developer and system administrator.

Vitaly is a graduate of the Belarussian State University.

ADDRESSING THE CHALLENGES OF CYBERCRIME INVESTIGATION WITH THE HELP OF OPEN SOURCE TOOLS FOR REMOTE FORENSICS

*Authored by
Vitaly Kamluk*

When investigating cybercrime, access to reliable, robust, flexible as well as user-friendly tools for remote forensics is a must. However, based on the experience of our team, in most cases investigators either don't have such tools, or only have tools with limited functionality. This significantly extends the length of the investigation and may sometimes even prevent the crime investigators from collecting some crucial evidence. In the latter case, remote locations combined with a lack of time and/or resources can mean that it is not possible to make a trip or hire local experts. Meanwhile, this problem may have a rather simple yet effective solution.

The solution would be a tool that allows a professional digital forensics specialist to connect remotely to a computer which carried relevant forensic images as attachments, or even original evidence in the form of hard drives infected with malware, and then to collect evidence in a way that would make it admissible in court. To the best of our knowledge, there is no tool commercially available that would allow for the remote acquisition of disk images, or triage, without either tampering with the evidence system or requiring the purchase of some expensive hardware. Perhaps it is widely believed that existing methods of cybercrime investigation work pretty well. But they don't. Here's why.

The challenges of cybercrime investigation in Darknet

Despite the fact that in recent years we have seen multiple successful cybercrime investigations, there are obstacles which investigators face on a routine basis. One major challenge is that more and more

cybercriminals nowadays use so-called Darknet services to create the backbone infrastructure for a crime. Darknet services (e.g. the Tor protocol, Blockchain-based solutions etc.) all operate in a way that is significantly different to the way "regular" web technologies work.

Based on our experience of running cybersecurity and cyber forensics training for law enforcement agencies (LEAs) around the world, the very concept of the Darknet-ecosystem itself has yet to be fully understood by operatives involved in cybercrime investigation. There is nothing surprising in this situation: in fact, a full understanding of how Darknet technologies work requires more time and practice than law enforcement agencies are ready to spend, because resources are limited, and cybercrime is only one of many types of crime that modern LEAs have to investigate. In other words, this is a very specific area, which requires a specific set of computer skills.

Another challenge is the fact that a suspect doesn't have a defined geographic location. When it comes to Darknet technologies, the task of identifying a suspect's geolocation becomes significantly harder than in cases where "regular" web technologies are involved. This is due to two main reasons: first, location-obfuscation technologies, like Onion-routing, make it more difficult for law enforcement agencies to identify the source of malicious code and the possible suspect behind it. Second, in many cases, it is just not clear under whose jurisdiction the computer of interest is located and what legal procedures must be followed by

an investigator in order to get access to the evidence.

Both issues are potentially solvable. But to do so in a reasonable amount of time the investigators need to have access to multiple computers involved in a cybercrime.

But this is a problem because, in most cases today “getting access to evidence” means “go to the exact location and get physical access to the infected machine”. This results in additional travel costs, increased time for the investigation, the need to address differences in legislation, etc. Investigators have to go to a remote location because, even when using most of the existing solutions for forensics, you need a trained forensic specialist in the place of interest to acquire the data and do triage analysis in the proper way. In most of the cases we have witnessed there were no such specialists available.

Actually, a lack of well-trained resources is not only about not having a specialist in a remote location who can set up a Linux system properly. It is potentially a much bigger problem and part of the overall problem of investigating cybercrime in the Darknet. Here’s why.

The new kind of investigators

First of all, based on our experience in assisting law enforcement agencies around the world, we can say that modern police officers working on cybercrime investigations come from police academies and schools, not from IT departments at universities. In many cases cybercrime investigation skills are something they acquire in addition to their main set of skills. Sometimes it is perceived as just another training course that, once completed will raise the professional level of the investigator forever. Additionally, commercial software businesses, which develop tools for cybercrime investigations,

are trying to adjust to this situation and are making tools that are relatively easy to use by a person with mid- to low- level technical skills. This approach can make the process of gathering and analyzing evidence ridiculously simple, down to pushing to buttons: “Acquire” and “Analyze”. That doesn’t help when it comes to some custom and sophisticated cyberattack, where the investigator has to go beyond standard procedure and fully understand what is happening under the hood of the analysis software.

What I mean by this is that existing tools more or less cover the needs of current cybercrime or a regular crime investigator, but, based on our analysis of the direction in which the cybercriminal ecosystem is moving, this will not be the case in the future. Even today criminals and sophisticated cyberespionage actors are using software, encryption protocols and other components that are not widely used, and are not researched well enough to develop a standard forensic tool for all of them. In the future the situation will become worse, because ever more diverse software will appear and it will be simply impossible to create a plug-and-play product which would allow data from any source to be processed effectively. Or it would cost enormous sums of money to buy and support.

In other words, there should be changes in the way cybercrime investigators are trained and which tools they use. Today a cybercrime investigator is capable, on average, of understanding the basic terminology of cybersecurity and cybercrime, and is able to translate this terminology into language which will be understood by lawyers, prosecutors and judges. Most of the technical job of collecting digital evidence is done either by third party cybersecurity expert or by a commercial software solution, or both.

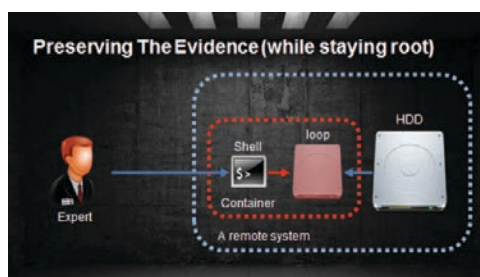
Tomorrow this level of skills will not be enough. The cyber-police officer should be familiar with core software principles, such as OS architectures, software frameworks, network protocols, file formats, compression and encryption algorithms and reverse engineering. Ultimately police officers should be able to code and create their own tools, or patch existing ones to suit their needs. Last but not least, cybercrime investigators should have access to tools, which would allow them to work remotely from any location, flexible enough to be useful in the investigation of crimes conducted with any kind of software. And this is where open-source technologies might be of help.

BitScout – the concept of a universal digital forensics tool

BitScout is a set of software based on open source code, which allows for trusted remote digital forensics and the collection of guaranteed untampered evidence. It gives an investigator the ability to conduct remote forensics operations. We created it for internal use while doing a routine cybercrime investigation.

It is well known that a proper cyber forensics procedure should not allow any hard drive disk (HDD) modification on the computer that is being examined. When an investigator has physical access to the computer, this requirement is addressed through the use of special equipment for creating a copy of the HDD. But when it comes to remote forensics analysis, the investigator might have shell-access to the system with the HDD evidence attached. This type of access allows the investigator to conduct arbitrary modifications on the HDD under examination. Theoretically, there is a question mark over the legitimacy of evidence collected in this way, because the investigator could have malicious intent or simply make a mistake and modify or even destroy the original evidence data. Interestingly enough, current

commercial software solutions that we are aware of do not solve this issue completely. When they are used for a remote forensics procedure, the investigator is considered by default as a totally trusted user.



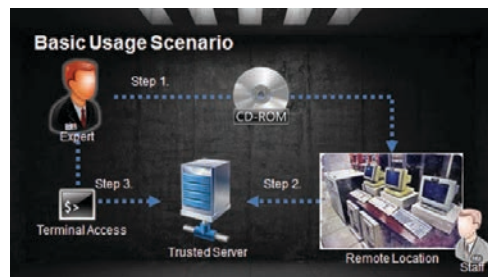
This is not a perfect situation, but luckily it can be improved. For example, a forensics investigator using BitScout while having root level access does not touch the evidence HDD at all. Instead the investigator accesses the virtual HDD device of interest in a special isolated container where he has virtualized full root access. This feature allows for full spectrum research of the hard drive (including installing additional software from public repositories) and at the same time guarantees that the data on the real hard drive is not modified. All possible changes made to the virtual HDD will not make it to the evidence hard drive and will be discarded when the system is shutdown. Implementing copy-on-write technique for such virtual HDDs makes this possible.

Moreover, certain types of cyber forensics analysis may require modification to the hard drive. This procedure is a must when it comes to the dynamic analysis of the machine under investigation. In order to reconstruct the malware behavior within a reasonable time it may be mandatory to launch it on the exact system environment it has infected. This is needed in order to find out which actions the malware performs, what servers it connects to etc. But the launch of malware

on a computer under investigation would inevitably lead to additional changes on its hard drive and may potentially destroy valuable evidence. When an investigator has direct physical access to the computer, this may be worked around by making a forensic copy of the HDD with the help of special equipment or software and then launching it on a dedicated physical or virtual machine. However, when it comes to remote forensics, the investigator may have no choice but to do these procedures on the hardware of the attacked PC, and as a result the content of its hard drive would be modified.

We encountered this problem several times during our work, and at the end of the day we've come to a solution in the form of a special feature of BitScout, which maps the virtual HDD to a remote trusted server or even to the computer belonging to the forensic investigator. Therefore the investigator can start a system with a virtual machine, observe the behavior of malware without the risk of changing the original evidence disk.

Last but not least, in order to deploy and launch tools that would allow for remote digital forensics, sometimes it is necessary to have a system administrator with advanced computer skills. As we explained earlier, this is not always an option. That is why BitScout is built in such a way that a person with basic computer skills would be able to just download a distributive, burn it to a CD or USB storage disk and launch it on the computer of interest without the risk of tampering with the evidence.



The software would then automatically connect to a trusted relay server and provide the investigator with access to the container the virtual HDD will be attached to.

The full list of BitScout features is as follows:

- Disk image acquisition with non-skilled local staff.
- Train people as you go (shared terminal session).
- Transfer disk image or part of it to your lab.
- Remote Yara or AV scan of an offline system.
- Extract, search, examine any registry keys, i.e. autoruns, services, etc.
- Remote file carving.
- Remediation of the remote system (cleaning from malware) if access is authorized by the owner.
- Remote scanning of other network nodes for infection (useful for remote Incident Response).

One of the key features and biggest advantages of the BitScout tool is that it is fully built on free and open source software, which means that it doesn't require any financial investment, license fees etc. What's more important, thanks to the public availability of the vast majority of the components and the compatibility of BitScout with commonly used hardware, this tool can be adjusted to the particular needs of an investigator, and, of course, improved and upgraded with additional features and custom software.

Preparing for the future

There is no perfect software tool that would solve all the issues which the investigation of cybercrime brings with it. But from our perspective, BitScout is a step in the right direction. It is no secret that nowadays even the investigation of a traditional crime often has lots of things for cyber forensics specialists to look at, and in the future this process of the fusion of different types of crimes will continue. Therefore the process of crime investigation should evolve as well. With proper training for investigators and reliable and flexible tools in place, cyber forensics experts and law enforcement agencies around the world will be able to effectively address the crime problem now and in future.

**Nick Savvides**

Information Security Specialist & Strategist
Symantec Corporation

Nick Savvides is responsible for Symantec's Cyber Security Strategy across Asia Pacific and Japan. In this role, Savvides' charter is to provide local market insights that influence global strategic planning and product development.

Savvides works also with organizations and governments to develop their cyber security strategies and solve complex business problems. He has worked on some of the largest business information security projects in Australia, affecting the way many Australian's interact with their employers, banks and governments.

An information security expert, with approximately 20 years experience, Savvides has spent the last 10 years at Symantec in various product and sales engineering roles. He has presented at more than 60 conferences, contributed to many high profile panel discussions and regularly appears in the media on cybersecurity related topics.

Savvides is an active member of the IT Security community and a member of a number of industry bodies. He is a Science graduate of The University of Melbourne.

OUTSMARTING INTELLIGENT CYBER SECURITY THREATS WITH MACHINE LEARNING

*Authored by
Nick Savvides*

Within the lifetime of many of us, the idea that machines could learn things that humans didn't specifically teach them was the stuff of science fiction. One skim through Netflix will uncover movies of evil computers plotting to take over the world. Isn't it interesting that now when we have actual artificial intelligence and machine learning as part of daily life, one of its key purposes is protecting people and property? At Symantec, the largest cybersecurity company in the world, we see over 10 trillion security events per year and more than one million pieces of malware a day; this is an unrivalled amount of data and the ability to understand it, process it and turn it into actionable intelligence is impossible to do using humans and traditional systems alone. This led us to develop and experiment with new technologies to tackle the scale problem, with Machine Learning and Artificial Intelligence being a key focus. This paper will discuss how these technologies have evolved and how they are applied in a cybersecurity context.

Machine Learning and Artificial Intelligence are closely related, although there are distinct differences. Machine Learning allows systems to learn from their inputs and experience without being specifically programmed, while Artificial Intelligence requires a machine to perceive and imitate human behavior. Consider a self driving car: the system that identifies pedestrians is Machine Learning, while the whole car driving to and from a destination a dealing with all aspects is Artificial Intelligence.

Although we may be a long way from Star Trek's conversational computer, there is no doubt that machines are learning and systems are getting smarter. In the self-driving car example, despite

many high-profile errors, more than 10 million cars with some self-driving features will be on the road by 2020. Singapore has recently kicked off the world's first driverless taxi trial in Singapore, pioneering a technology that is set to revolutionize the way we travel. These IoT-connected and automated vehicle systems can free up travelling time for commuters, allowing them to relax or work on-the-go, amongst other benefits.

While today's applications in digital assistants, a la Siri and friends, data mining, machine vision and industrial applications, might seem amazing, the reality is that we are at the infancy of Machine Learning and Artificial Intelligence. In reality, while these concepts have existed for 60+ years, it is really only in the last 10 years that sci-fi like advances have been made.

In terms of cybersecurity Machine Learning and Artificial Intelligence offer us a new opportunity to act as a force multiplier. The sheer scale of the threats, devices and networks that are operated today make it impossible for humans and traditional systems to scale to understand, to correlate and to connect. As discussed earlier, Symantec collects more information than any single system or human could understand and this problem is only expected to get worse, as huge new networks of devices and systems roll out, each acting as both a source of attack, a target of attack and generator of information and logs.

Consider the volume of new connected devices in the IoT that will come online in the next few years. All of these these are potential vectors of attack; in fact Gartner forecasts that by 2020, more than 25 per cent of identified attacks in enterprises will involve IoT¹.

This is where we must turn to Machine Learning and Artificial Intelligence. We need these systems to act as our force multiplier, as the systems that ingest all that data and then tell only about the things we should care about and act on, making our security analysts more productive.

To date, the cybersecurity application of these technologies has really been limited Machine Learning focusing on three things: threat detection, anomaly detection and user behavior analysis. Artificial Intelligence has yet to make a big impact on cybersecurity but this is likely to change over the next few years, as the technology matures.

Let's take threat detection as an example: in this scenario we entrust the Machine Learning system to be able to examine a new unknown file and determine if this file poses a threat. To do this it must learn by being show previously known bad files (convicted files), the more samples it sees, the features (attributes, components, behaviors) of those samples it sees, the more likely it will be able to detect and convict unknown files. This is a continuous process of self improvement; new results, when validated, feed the machine and continue to improve it. The machine and the data it is trained on are completely intertwined.

If we look at anomaly detection, this problem starts to become even more complicated. It requires the system to examine patterns of behavior and automatically build profiles from what it sees. This could be in closed system such as a self-driving car, where the system observes all of the components inside a vehicle and how they talk to each other and builds a baseline model for what is normal. When something outside of that model occurs it's flagged as an anomaly. The ability for anomaly detection on open systems such as the internet becomes extremely difficult due to the availability of data, as it can only

be truly effective if a large amount of data is sampled. At Symantec, we take advantage of our telemetry that comes from hundreds of millions of systems to achieve this.

These two things allow us to build tools that let us stay ahead of the cybercriminals. Threat Detection lets us discover their new unknown malware, while Anomaly Detection allows to see if a network or system has been compromised and if it warrants further investigation. Our security solutions imbued with machine learning can detect anomalies and outsmart intelligent threats, protecting us in instances where we are more susceptible but where do we go from here?

As more businesses embrace digitization, the way we protect ourselves must also evolve and there is a critical need to stay proactive against threats, instead of reacting to them. With the emergence of Artificial Intelligence, we may just be able to stay one step ahead of cybercriminals.

Eventually we will need to be able to build intelligent security systems that can not only learn faster than threats can present themselves but also be predictive of new attacks. It is foreseeable that a cybersecurity Artificial Intelligence, could observe all the outputs from Machine Learning models, looking at threats, anomalies and even current affairs news, and detect that an attack is about to happen. This would be an amazing force multiplier for our sophisticated cybersecurity centres, making analysts even more productive.

For example today, a security analyst will benefit from the big-data, analytics and machine learning that goes with modern security systems but needs to blend that with their understanding of the threat landscape. They need to follow blogs, understand the political landscape, understand the profiles of

the threat actors and even more challengingly navigate the dark web. Extracting features from files and understanding anomalies are simple tasks compared to this but it is possible for example to build Machine Learning models that understand natural language. Think of digital assistants, as they become more powerful and understand what you are asking from them, the same capabilities can be adapted to a cybersecurity role, at scale. Machines could scour the dark web and rather than looking for key words, understand and interpret what is being discussed, in any language, and feed this into Artificial Intelligence incorporating it with all the other Machine Learning output leading to perception and ultimately detection and production. This might sound fanciful, but 10 years ago many of things we take for granted today were purely science fiction.

While the idea of machine intelligence is ancient, its real implementation is recent. As compute power has dramatically increased while shrinking in size, increased memory and the quantity of data available, AI and machine learning are growing exponentially. Every time we buy something online, make a deposit or take out money from an ATM, glance at an ad, or turn on the faucet, intelligent machines are protecting us. It may not be as great a story as machines ruling the world – but it helps us all sleep better.

¹ <http://www.gartner.com/newsroom/id/3291817>

**Nils Andersen-Röed**

Operational Specialist / Project Leader
Darkweb Team
Dutch National Police

Nils Andersen-Röed is an Operational Specialist and project leader for the recently started Darkweb Team of the Central Unit of the Dutch National Police. One of the main goals of this team is to impair trust in Darknet markets and anonymity and security on the darkweb in general. Andersen-Röed joined the Dutch National Police in 2011 and, after receiving his Master of Criminal Investigation degree, has been working as an investigator and counter-thinker at the National Crime Squad. Prior to joining the National Police he received his Masters degree in Psychology and was working as a network professional in the private sector.

DARK WEB INVESTIGATIONS - AN OVERVIEW FROM THE DUTCH POLICE

*Authored by
Nils Andersen-Röed*

The dark web is the part of the deep web (the non-indexed part of the internet) where people can surf anonymously. The dark web consists of several different Darknets such as Tor (The Onion Router), Freenet, I2P (Invisible Internet Project), Openbazaar or Zeronet. Access to the dark web needs a special browser.

Tor is currently the most commonly used network, and it can be accessed by using the Tor Web Browser which allows the identity and the location of the user to stay anonymous due to the use of a multi layered encryption system. It is also possible to host services on the Tor network, known as the Hidden Services. If the server of the Hidden Services is configured correctly, both the physical location of the server and the identities of the users remain hidden.

The Hidden Services are commonly used to host Darknet markets. Vendors and buyers on these platforms can contact each other in order to trade (mainly illegal) goods, such as drugs, weapons, counterfeit documents or money, cybercrime-tools, or stolen credentials. Communication between vendors and buyers usually takes place via PGP (Pretty Good Privacy) encrypted messages and the purchased goods are paid in cryptocurrency like Bitcoin, Monero or Ethereum. In addition to the vendors, administrators of Darknet markets also earn a percentage (usually 2 to 5 percent) for each sale that is made on their market. Currently, the most popular Darknet markets are Alphabay, Valhalla, Dream Market, Hansa Market and Acropolis Market.

In the last couple of years, Darknet markets have grown substantially and the yearly revenue of Darknet markets is estimated to be about several hundreds of millions of

dollars. According to a recent study by RAND Corporation (2016)¹, revenues from Dutch vendors are by far the largest on a per capita basis compared to vendors operating in the United Kingdom or the United States, and they specialized in selling ecstasy (MDMA)-type drugs and stimulants. Dutch police investigations have also revealed that in addition to selling drugs on Darknet markets, some online vendors agreed to face-to-face meetings with their buyers in order to sell larger quantities of drugs in the physical world. It is not known how often these kind of meetings take place and the quantities that are being sold.

Besides buying and selling drugs, it is also possible to buy weapons and explosives on Darknet markets. Other Hidden Services consist of websites that offer assassination services, money laundering services, child pornography or terrorism-related information.

Due to the recent growth of illegal Darknet markets, the Dutch National Police have formed a dedicated dark web unit in order to combat crime on the dark web, impair trust in Darknet markets, and overcome the anonymity and security on the dark web. In the recent years, the Dutch National Police have investigated over 50 dark web related cases. About half of the cases were drug related, and about a quarter of involved the purchase of weapons or explosives. These investigations revealed that vendors located in the Netherlands are typically selling drugs, while Dutch buyers are mainly purchasing weapons and explosives. These investigations were launched either due information received from foreign law enforcement agencies, or leads on suspects identified by the investigative units through Big Data analysis or the interception of shipped parcels.

The trading of illegal goods on the darknet can be divided into four different phases: production; online vending of the illegal goods or substances; transportation; and financial transaction in which virtual currency is converted to fiat currency or goods. Police investigations can focus on all four phases in order to identify vendors. Several tactics and strategies can lead to the successful identification of suspects, mostly through the combined use of digital and traditional investigative methods.

For example, investigators from the Dutch National Police have successfully identified a vendor through the use of undercover tactics of acting as a buyer to make test-purchases while concurrently infiltrating the forum of the Darknet market to become a trustworthy partner to the vendor. After gaining enough trust, a face-to-face meeting was arranged where the identity of the vendor was revealed. Several other cases were solved through the analysis of text messages - between vendors and customers - which were gathered during previous police operations. Some of these messages contained useful details about the location of the vendor, meeting places, telephone numbers, PGP keys, information about their social life or information about their appearance. In one case, the combination of the information on the location where the vendor met with his customers and a news article about the vendor's family on a local news website in the same region led to the successful identification of the vendor.

The Dutch National Police are also actively working together with the parcel delivery services. When packages with illegal substances are detected during parcel inspections, their return addresses or track and trace codes are investigated in order to find out which postal offices the parcels were sent from. By tapping on CCTV surveillance and employing physical surveillance at the neighborhoods of these

postal offices, the identities of the vendors were successfully established. A dedicated post parcel intervention team has been formed to focus on the investigation of such intercepted parcels.

The police can also combat Darknet related crime by focusing on the money trail of illegal transactions. For example, the Dutch National Police have successfully identified a bitcoin-to-cash exchanger that was active on the bitcoin exchange platform localbitcoins.com. Tactics that were used consisted of a combination of bitcoin transaction analysis, and traditional investigative methods such as analyzing CCTV footage and investigating traditional banking transactions.

Besides focusing on identifying vendors or criminal bitcoin exchangers, the Dutch National Police are also developing new methods to identify the physical location of Darknet markets in order to target the markets directly. Although previous take-downs of Darknet markets have produced valuable intelligence, new markets have emerged to fill the gap and enable vendors to continue with their businesses. Therefore, the Dutch National Police are also working on developing innovative methods to tackle this problem.

In October 2016, the Dutch National Police and the Dutch National Prosecution Service have launched a Hidden Service on the Darknet. The Hidden Service (<https://politiepcvh42eav.onion>) features information on the detection and prosecution of many large vendors who operated on Darknet markets. It also points out that the buyers of illegal goods on the Darknet are not as anonymous as they might think. In sum, the level of difficulty in Darknet investigations is comparable to traditional investigations if a combination of digital and traditional investigative methods is used. However, the Police's successes are

contingent on the criminals making mistakes. Fortunately, the internet never forgets when criminals make mistakes.

¹ Kruithof, Kristy, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso and Stijn Hoorens. Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1607.html.



Vasilios Mavroudis
University College London

Vasilios Mavroudis is a doctoral researcher in the Information Security Group at University College London. He studies security and privacy aspects of digital ecosystems, with a focus on emerging technologies and previously unknown attack vectors.

His recent publication on ultrasound tracking received wide-spread attention and is considered the seminal work on the security of that ecosystem. Vasilios is currently working towards the standardization of ultrasound communications, and designs extensions of his previous attacks. Moreover, in cooperation with industrial partners, he has recently prototyped a high-assurance hardware architecture, that maintains its security properties even in the presence of malicious hardware components.

In the past, he has developed auditing tools for the Public Key Infrastructure of Deutsche Bank and participated in an international consortium studying large-scale security threats in telecommunication networks. Furthermore, he has cooperated with UC Santa Barbara in several projects, including a detection system for evasive web-malware.

Vasilios holds an Information Security MSc from UCL, and a BSc on Computer Science from University of Macedonia, Greece.

UNMASKING CRIMINALS IN THE DARK NET USING ULTRASOUNDS

*Authored by
Vasilios Mavroudis*

Executive Summary

In the last few years, unlawful activities in the Darknet have become a major challenge for law enforcement agencies, as criminals use them increasingly often, knowing that identification of individuals is far from trivial. To address this problem, we introduce a new set of law enforcement tools that can be used to uncover the identity of criminals in anonymity networks and services (i.e., the Darknet). These tools are highly effective, and are based on an emerging digital ecosystem that uses inaudible audio signals to link the different devices owned by a user. Compared to existing solutions, whose success-rate in real-life conditions has been proven quite limited, our techniques do not rely on vulnerabilities in the darknet software or design. Instead, they utilize the capabilities provided by the ultrasound ecosystem to create a high-accuracy link between the anonymous identity of the criminal and his real one.

Currently, Tor is the most popular anonymity network that enables users to both browse websites and host their own services, while hiding their real identity. Due to its popularity, Tor handles the great majority of “anonymous” traffic and is estimated to host approximately 30,000 hidden services. Not surprisingly, Tor and the darknet in general, serves as a major hub for various kinds of criminals, as it allows them to conceal their activities, and more importantly protects their identity from law enforcement. This allows criminals to maintain pseudonymous Darknet identities and use them to build a reputation in their underground community. Such behavior is most commonly observed in Darknet trading venues, where the users buy and sell illegal goods and services and try to build and maintain reputable profiles to increase their revenue.

Unfortunately, even when law enforcement traces these illegal platforms, the identification of the criminals remains a challenge. In this context, our techniques realize a new way for authorities to deanonymize criminals who visit Darknet websites and resources. To achieve that we developed a set of tools that use popular ultrasonic applications to transmit a unique identifier from the “anonymous” device used by the criminal, to nearby devices that have not been anonymized. For instance, cross-device tracking and proximity marketing application deployments can be used to trigger specific functionality in the criminal’s smartphone, by remotely injecting specially crafted inaudible tags. Moreover, it should be noted that in most cases the users are not aware that their device is listening for ultrasounds, as this functionality comes as part of a third-party framework incorporated in the app. In addition to these, we also extended our techniques to operate in an offline fashion, so that they can be used in physical, real-life encounters, where connectivity is not always assumed.

All in all, the ultrasound ecosystem already features a wealth of applications and is expected to expand further in the next two years along with the number of participating users, which we currently estimate to be at least few million. Consequently, the coverage and the effectiveness of these techniques are expected to also increase with the number of devices listening for ultrasounds, thus providing a robust way to uncover criminals residing in the Darknet.

**Maria Vello**

Certified Information Systems Security
Professional (CISSP)
Chief Operating Officer
Cyber Defence Alliance

Ms. Maria Vello, CISSP, joined the Cyber Defence Alliance (CDA) as Chief Operating Officer in April 2016. Prior to this she was CEO and President of the NCFTA (National Cyber-Forensics & Training Alliance) for three years. Maria has been recognized by the FBI Executive team and FBI CIRFU for her exemplary service, partnership and contributions to the Cyber Division. She has been recognized by the NCFTA for her exemplary leadership, dedication and unparalleled passion for the NCFTA mission. Awarded the AT&T Leaders Council award for being in the top 2% at AT&T, she was the also the number one Regional Security Manager at Cisco Systems, number one AT&T Sales Manager and she was also named to the top ten women in Cloud in 2014. Maria brings a wealth of experience in trust-based collaboration, information sharing across industry, law enforcement, government and academia to proactively detect, protect, deter, dismantle and stop cybercrime or threats. She has effectively led teams to leverage cross-sector resources and threat intelligence to more effectively analyze, correlate and attribute critical real-time intelligence against emerging cyber threats and deliver actionable intelligence to both industry and law enforcement.

TACKLING CYBERCRIME - ONE CHALLENGE AT A TIME, COLLECTIVELY AND COLLABORATIVELY

*Authored by
Maria Vello
Michael Shoukry*

The Cyber Defence Alliance (CDA), is a non-profit public private partnership focused on the collective and collaborative sharing of information and intelligence at an industrial level to fight cybercrimes/threats and provide actionable intelligence for our members and partners. The CDA has been able to pave the way for an unprecedented level of information sharing to tackle cybercrime. The CDA has proven, it is only through earned and sustained trust in a purpose built environment that you will truly and share at the levels required to be effective in this war on cyber threats/crime. Through this unprecedented and real-time sharing the CDA has been able to demonstrate that by collectively and collaboratively working together we can accelerate our knowledge, innovation, capabilities and preparedness. We also know that no one tool can enable the transformation of data into intelligence and ultimately into action. However through the application of collective efficacy model within a purpose built trust environment, the CDA has been able to combat cybercrime. The pace of the cyber threats are astonishing and this is a systemic and global problem. In today's ever changing threat landscape the only way to tackle significant and highly distributed threats is to accelerate our pace through a trust and unified model, to pool our resources, information, and knowledge, globally.

Taking the above approach is not always the easiest as there are challenges of differing legislation, policies, and governance models across countries, organizations and borders. In addition, the laws around extradition, prosecution and law enforcement agencies work together can be challenging and cumbersome. The Mutual Legal Agreement Treaty (MLAT) process is not always conducive or fast enough in cyber, especially when being expedient is critical. However, through

this unified, collaborative trust model, the CDA has proven that this trust model can stop imminent attacks before they happen, identify malicious actors, and ultimately arm law enforcement with the necessary intelligence to dismantle criminal enterprise organizations, their infrastructures, and arrest malicious actors and seize their assets for long term impact.

Cybercrime can have devastating impacts on organizations, individuals, economies, and governments. The threat landscape is constantly increasing, the problems are constantly evolving, the threats are increasing from the basic spam, malvertising, Nigerian scams, social engineering, phishing scams, to extremely sophisticated exploitation of vulnerabilities leading to ransomware, zero days and much more. But why does this gap exist and continue to widen? And how can we collectively shrink this rapidly widening gap and fight cybercrime at scale?

Why does the gap exist?

- Is it a lack of education or knowledge;
- A deficiency in understanding the risks;
- A lack of sharing;
- A lack of resources, skills, expertise;
- A lack of tools to combat such threats;
- An increased number of vulnerable systems/code;
- Amount of sophisticated exploits and exploitation tools leaked;
- Innovative threat actors;
- New emerging technologies and capabilities (IoT devices, easily accessible cloud computing systems, etc.);
- A gap in laws;
- The penalties/implications of getting caught are not severe enough;
- A gap in enforcement or law enforcement capabilities to combat such crimes;

- Legislation and regulations have not kept pace with the times or adverse implications of the internet;
- The darknet;
- Off-line secure encrypted communications, (obfuscation)
- We could go on, the list is immense;
- Or is it simply all of the above?

When we look across the above items as to why this gap may exist, the answer becomes somewhat overwhelming, especially since many are difficult to measure through tangible means at a global level. However, the only clear answer is this solution is highly likely decentralized across both the private and public sector and across many industries and across the globe. By reflecting on past successes of both traditional law enforcement (drug cartels, terrorism, crimes against children, etc.) and cybercrime (botnets, silk road, criminal forums), we quickly recognize that solving this global problem requires international collaboration through private-public partnerships.

Many cybercriminals are opportunists always looking to take advantage of the circumstance to exploit easy targets, the classic example of this is “an older person looking for love”, or a simple phishing email, both of these have been around for over a decade and are still being employed by malicious actors. But why do these attacks continue to get used? These attacks are only continuing to be used because they are successful. If such attacks were not successful, malicious actors would quickly pivot to the next opportunity. Of course as new opportunities for more sophisticated attacks arise, the attackers will quickly begin adopting them, for example in more recent cases, attackers leveraged vulnerabilities in software to build a wormable ransomware and impacted thousands of people (WannaCrypt/Wannacry). Cybercriminals are always looking to enhance their business model and as new innovations

emerge, criminals utilize technology just as those security practitioners and general technologists in our industry do to become more profitable, and scale their criminal enterprise. Enterprise groups are the poster child for why and how information sharing can be extremely effective. They have dramatically improved their pace, innovation, knowledge and capabilities to elevate their game and gains. They have the best sharing model on the planet – we can learn from them. They know us better than we know ourselves, they know our thresholds, limits, systems. They know our rules and regulations better than we do, when we come out with new rules, regulation, best practices they do an exceptional job of communicating that information out to each other. One example is NIST in the US. When NIST was finally published, within days, it was made available in the underground market to all of the cyber criminals, translated in multiple languages.

The darknet/darkweb “marketplace” has certainly played a role in increasing the pace and magnitude and escalation of cybercrime and it will for a long time. However, it is getting increasingly difficult to leverage it to gain actionable/evidential intelligence for some of the very serious organized crime groups and get into the vetted forums. You have to pay to play with the advanced, experienced, sophisticated groups and forums. You have to demonstrate your own value and actually commit the crime in a number of the groups. Even in the dark criminal marketplace, there are ratings for trust. The ability for criminals to take conversation off-line into private secure chats, secure communications and obfuscate themselves is far too easy.

As new tools and technologies emerge, criminals will quickly look to adopt it and leverage it to enhance their operations. This is shown with how new innovations such as TOR, P2P, blockchain, anonymization services,

encryption, secure communication software etc. are being used by cybercriminals.

Criminals have used the above technologies and others to develop their own Software packaged in an “as a Service” model (Also referred to as Ransomware as a Service), offering business analytics dashboards, and a full platform for any novice threat actor to launch an attack. With the increased accessibility of these criminal services, the attacks will continue to be on the rise. By attempting to go after each one of these tools or services, we quickly realize that this becomes a game of “Whack-A-Mole” that won’t lead to the desired long-term impact.

This global problem only gets more challenging as we take a look at varying laws, regulation, and a decentralized law enforcement eco-system. Varying data and privacy laws, regulation, and a lack of consensus among lawmakers adds a whole new complexity to this challenge. While there is no dispute that privacy, laws and regulation are a necessity, we must collectively agree to streamline the processes and develop balanced and flexible regulation to support the fight against cyber criminals who have a total disregard for the law and simply do not adhere to governing principles. It is critical that we preserve the balance in maintaining a safe, secure, and transparent cyberspace, and a complex challenge such as this requires a collective approach that is built on trust.

The Internet is borderless, and cybercriminals use this to their advantage.

Cybercriminals use laws and any regulations that we place on information sharing to their advantage. It’s imperative that we maintain a balance to protecting the privacy of non-malicious individuals; it’s also critical that we collectively agree on policies and legislation that allows the exchange of information through public-private channels for the right reasons and intent.

Through education, situational awareness, changing our behaviors, truly sharing our resources, information sharing, public-private partnerships and securing our systems across the globe, only then will we be able to put a dent in cybercrime and cripple cybercriminals. By raising the cost of committing crimes/ reducing their return on investment, increasing the severity of the penalties, increasing the probability of getting arrested and prosecuted, and lowering the likelihood of successful malicious exploitation, only then will the scale begin to tilt in our favor.

Should there be norms, how do we get these done on a global basis? We have only discussed the challenges around cybercrime, what about Nation States, the political implications and our inability to extradite in some countries? There are many areas to address and we will over time, but time is of essence. It is not just financial aspects of cyber we should be troubled about and focused on, but also our intellectual property, patents, research and development, mergers and acquisitions, ability to influence countries elections, recruitment of people and more importantly the ability to distinguish between the truths, what is real, what is fact.

This fight against cybercrime is a threat to our economies, critical infrastructure, and attacks can lead to devastating impact. We must come together, unify our forces, pool our resources, knowledge, to increase our preparedness and make forward progress in raising the difficulty for criminals to operate in cyberspace. Every one of us has a moral obligation and plays a critical role in helping to neutralize cybercrime/threats and focus on building a safer cyber future. There is not one company, agency, or country that can fight this war alone.

The CDA Team

**Benjamin Ang**

Senior Fellow

Center of Excellence for National Security
(CENS)

S. Rajaratnam School of International Studies
(RSIS)

Benjamin Ang is a Senior Fellow at the Center of Excellence for National Security (CENS), S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. He leads the Cyber Programme of CENS, a team whose research areas include international cyber norms, cyber deterrence, cyber state governance, hybrid warfare and influence operations, cybercrime, smart city cybersecurity and governance, data privacy, and cyber issues in artificial intelligence. He also serves on the Executive Committee of the Singapore Chapter of the Internet Society, the international non-profit organization that is the trusted source of leadership on Internet policy, technology standards, and future development.

He draws on varied experiences as a litigation lawyer in one of Singapore's largest firms, CIO in a multinational professional services firm, legal counsel in media and technology companies, and as a technology consultant. His current publications and commentaries on cyber policy issues can be found at <https://www.rsis.edu.sg/profile/benjamin-ang/>

TACKLING TRANSNATIONAL CYBERCRIME WITH MUTUAL LEGAL ASSISTANCE

*Authored by
Benjamin Ang*

International challenges of cybercrime

A recent INTERPOL investigation identified nearly 9,000 servers in Southeast Asia that are being used for cybercrime, including command-and-control for malware, launching distributed denial-of-service (DDoS) attacks, spreading ransomware, and sending spam, with victims and suspects in China, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

There are also documented cases of cybercriminals based in Romania, Estonia, Lithuania, and Russia, who have committed large scale crimes ranging from ‘phishing’ (sending millions of email luring users to fake banking websites to steal their banking passwords), theft of credit card numbers and ATM PINs, computer intrusion, wire fraud, illegal appropriation of money, and installing malware that intercepts bank account passwords. In all of these cases, the criminals committed their crimes without ever physically stepping into the same country as their victims. They illustrate how global technology can be used for committing criminal acts with a transnational reach, posing a huge challenge for local law enforcement. Fortunately, there are international legal instruments that local law enforcement can use to address this challenge.

Many countries have passed legislation that provides jurisdiction over cybercrime activity affecting their citizens or property, even if the criminals are located outside the country borders. However, merely criminalizing transnational cybercrime is not effective. Successfully combatting cross-border cybercrime, however, requires more than just criminalization. Success requires effective international cooperation.

Unfortunately, International cooperation in cybercrime cases comes with well-known challenges. Foreign authorities may be reluctant to recognize legal traditions and systems, particularly if they are requested to assist in a manner which is different from their own national law or principles. States are also naturally reluctant to transfer their citizens to another state for criminal prosecution. Some countries rely upon a tradition of non-intervention and may view investigation assistance as burdensome or intrusive absent a treaty for cooperation.

Conventions, Treaties and Mutual Legal Assistance

International law enforcement cooperation can be either formal or informal. Formal mechanisms include bilateral or multilateral treaties for mutual legal assistance. This is the process by which States request and provide support in criminal cases. The largest global cybercrime cooperative agreement is the Council of Europe’s Convention on Cybercrime (“Budapest Convention”). Article 22(1)(a) of the Budapest Convention requires signatories to recognize computer crimes that are committed in their territory, while Article 23 requires signatories to provide cooperation to the widest extent possible, including collection of evidence. Other important instruments are the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime within ECOWAS, Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information, Shanghai Cooperation Organization (SCO) Agreement on Cooperation in the Field in International Information Security, African Union (AU) Draft Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa, and League of Arab States (LAS)

Arab Convention on Combating Information Technology Offences.

In addition to the Budapest Convention, individual national Mutual Legal Assistance Treaties (MLAT) treaties have established streamlined procedures for rapid cooperation between law enforcement authorities. Time is of the essence in combating cybercrime, as computer evidence is highly volatile and easily destroyed. These treaties provide for expedited preservation of evidence and disclosure of stored computer data. They may also provide for mutual assistance in the real-time collection of traffic data, and the interception of content data.

To implement these forms of assistance promptly, states also agree to designate points of contact who can be reached on a 24/7 basis. Other contact resources include the UNODC Online Directory of Competent National Authorities, Commonwealth Network of Contact Persons, European Judicial Network, and Eurojust.

Limitations to Mutual Legal Assistance

Mutual Legal Assistance treaties are still not a magic bullet, as many agreements and domestic legislation place limits on mutual legal assistance. Some of the situations where assistance will not be provided include acts which are political offences, acts which are not criminal offences in the assisting state, and instances where implementing the request could violate the assisting state's sovereignty, security or order.

Despite these limitations, law enforcement agencies in many countries have found success in transnational cooperation to combat transnational cybercrime. The most well known examples are US law enforcement officials who have successfully cooperated with their counterparts in Lithuania, Estonia, Spain, and Bulgaria, in arresting a number of

cybercriminals, and in many cases extraditing them to the USA for trial. These, and many other unsung heroes, are good indicators of the effectiveness of cooperation and international legal instruments in the battle against transnational cybercrime.

STRONGER ENCRYPTION OR WEAKER ENCRYPTION FOR PUBLIC SAFETY?

*Authored by
Benjamin Ang*

In the wake of terror attacks around the world, government leaders including those of France, the United Kingdom, USA, and Australia, have condemned strong encryption – the technology that keeps data and messages hidden from third parties – as hindering efforts to combat terrorism and crime. On the other hand, technology and security experts have criticised such calls to weaken encryption, arguing that weakening encryption would not only fail to prevent terrorism and crime, but would instead cause greater insecurity for the public.

The case for weaker encryption

From a technical perspective, any device or application that can be penetrated on demand is considered to have a ‘back door’ for entry. However, since the term has its baggage, this article will use the term ‘weak encryption’ instead.

Surveys in the USA have indicated that the public would favour weakening encryption if that would enable law enforcement to investigate and prevent terrorists and criminals from striking. One example would be messages that the Westminster attacker Khalid Masood apparently sent on WhatsApp just minutes before he launched his assault that killed four people. Presently these messages are encrypted and cannot be accessed even by the WhatsApp company.

Officials argue that such terrorist attacks would be easier to prevent if authorities could penetrate encrypted services like WhatsApp, just as they used to listen in on telephone calls or steam open letters and read their contents. The safeguard would be that the police or other authorised agency would need a warrant through the proper channels.

In this light, it appears perplexing that Apple

and Google announced that their iPhones and Android smartphones will be encrypted end-to-end by default i.e. all the data stored on the phone itself will be unreadable to anyone who accesses the phone without the device passcode, and that even they (Apple and Google) would not have access. Why would they do such a thing?

The case for stronger encryption

Firstly, it is argued if WhatsApp, iPhones and Androids have weak encryption, this would not deter terrorists. The terrorists who attacked Paris used prepaid burner phones, not encryption, to keep off the radar of the intelligence services. After the attacks, investigators found the phones with a detailed map of the concert hall and an (unencrypted) SMS messaging saying “we’re off; we’re starting.” Investigators found evidence that ISIS supporters are disinterested in using encryption to hide their web browsing activities, or to create a secure version of propaganda websites.

Terrorists and criminals who want to hide their communications will still have a wide range of strongly encrypted apps and tools, easily available from other developers. Signal, Telegram, Threema, and ChatSecure are only the tip of the iceberg. ISIS has apparently made its own encrypted messaging app called “Alrawi”.

Secondly, it is argued that weak encryption will expose confidential data (banking data, passwords, trade secrets) as well as critical infrastructure (banks, power grids, telecom), to risk. The US House Homeland Security Committee acknowledged in their report that creating a means for law enforcement to get access to the data stored in Google or Apple phones “would naturally be exploited by the bad guys—and not just benefit the good guys.”

The fundamental problem is that if one government can penetrate encryption to access a device, eventually so will malicious hackers, identity thieves, and foreign (possibly unfriendly or corrupt) governments, thereby actually enabling cybercrime and undermining national security. This happens because any encryption which can be penetrated therefore has a vulnerability, and cybercriminals have many nefarious ways to find vulnerabilities. One example is the ransomware attack named WannaCry that affected businesses, hospitals and governments of more than 150 countries, using vulnerabilities stolen from the National Security Agency, the USA's top spy organization.

One may trust one's own government to properly safeguard the ability to penetrate one's encryption, but one must also remember that every other government in the world will also have the same ability, because technology companies must grant access equally. When geopolitical conflicts arise, this would be detrimental to national security.

Thirdly, any security weakness in our increasingly complex network environments can be exploited by cybercriminals, to infiltrate critical systems like banking systems. When bank statements for Standard Chartered Bank's wealthiest clients were found on a hacker's laptop, they had been stolen not from the bank's highly secure servers, but from a less secure server at the company which prints the bank statements.

Particularly in the financial sector, encrypted communications provide confidentiality as well as authentication, which is required for secure transactions. Any cybercriminal who can penetrate encrypted communications will also be able to forge them.

Public safety

Even in other sectors, researchers keep finding malicious software that can shut down

electricity grids, pacemakers, and the brake systems of cars. As more devices like smart cars and smart homes become connected online, as part of the Internet of Things, it appears that stronger security everywhere, not weaker, is needed to protect public safety.

There may be technologies in the future that enable encryption to be penetrated safely. Perhaps (and this is wildly speculative) quantum cryptography, where the act of reading data encoded in a quantum state changes the state, would enable users to detect eavesdropping in quantum key distribution, even distinguishing between lawful authorities and cybercriminals or enemy states.

In the meantime, with the present state of technology, public safety is better served by encouraging technology companies to make devices and applications with stronger encryption, not weaker encryption.

**Tan Teck Boon**

Research Fellow in the Office of the
Executive Deputy Chairman
S. Rajaratnam School of International Studies
Nanyang Technological University,
Singapore

Teck Boon is a Research Fellow in the Office of the Executive Deputy Chairman, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His research covers smart cities governance, policy implications of emerging science and technology as well as inter-organisational cooperation and information sharing. He obtained his PhD from the Lee Kuan Yew School of Public Policy, National University of Singapore (NUS). He also holds a Master of Social Science from the Department of Economics, NUS, and a Bachelor of Science in Economics from the State University of New York, USA. Prior to joining RSIS, Teck Boon held research positions at both the Lee Kuan Yew School of Public Policy and the Department of Economics, NUS.

PITFALLS OF THE “INTERNET-OF-THINGS”

This article first appeared in RSIS commentary

*Authored by
Tan Teck Boon*

Synopsis

The global network of Internet-enabled sensors, devices and systems called the “Internet-of-Things” promises many upsides. But many IoT products are vulnerable to hacking. In the IoT age, it is vital to strike a balance between the risks and rewards.

Commentary

THE “INTERNET-OF-THINGS” (IoT) is a catchall phrase for the global network of Internet-enabled sensors, devices and systems that collect and share a vast amount of personal data. Wildly diverse and growing fast, the billions of IoT products out there right now include fitness trackers, medical devices, household appliances, mobile gadgets and even Barbie dolls. According to IT research company, Juniper Research, there are now more than 13.4 billion IoT products in use and by 2020, the figure will hit 38.5 billion.

Proponents contend that once we are fully immersed in IoT, the technology will engender myriad benefits. They claim that energy-saving IoT products will enhance our situational awareness and quality of life too through automation. For example, when a sleep tracker is connected to a smart air-conditioner and coffeemaker, the wearer not only wakes up to a freshly-brewed cup of coffee but also feeling totally refreshed because the temperature in his bedroom is synced to his sleeping pattern. So not only does the wearer of the sleep tracker know the quality of his sleep, he is also doing his part for the environment by letting the smart air-conditioner adjust the temperature accordingly throughout the night. As appealing as this high-tech option may sound, it is unfortunately clouded by serious cybersecurity concerns.

The Downsides of IoT

The biggest fear right now is that a large number of IoT products are susceptible to hacking. Indeed, many IoT products are resource-constrained, meaning that they do not come with firewalls, encryption/authentication and antivirus capabilities built-in. We install security protection into our smartphones, PCs and tablets; but doing so with the smart toothbrush or kettle may not be possible because they have limited computing power. Even if it were possible to patch IoT products with security upgrades after they had left the factory, it would be a logistical nightmare given their sheer numbers out there.

According to estimates from Hewlett Packard, a staggering 70% of IoT products currently in use are vulnerable. In a sign of things to come, penetration tests (or “pen-testing”) designed to uncover security vulnerabilities in IoT products have shown that it is possible to breach home Wi-Fi networks via IoT appliances. So hackers could in theory exploit weaknesses in everyday IoT products and work their way into corporate or government networks as employees bring their infected gadgets to work.

Sounds incredible but in 2013, we inched closer to this dystopian nightmare when hackers breached the database of Target and stole the credit card numbers of 40 million customers apparently by hacking the US retailer’s Internet-enabled heating and air-conditioning system.

Implications of a Cyber Takedown

In the worst case, hackers could take over or shut down major infrastructure networks throwing critical sectors like banking, transportation and telecommunications

into chaos. The consequences would be catastrophic. Or they might attempt to retrieve sensitive information stored in these networks. Bear in mind, IoT products collect a vast amount of personal data. Not just plain information like names, birth dates and contact details but revealing information like energy consumption patterns, geo-location data and lifestyle habits. To the untrained eye, this kind of information means nothing but in the hands of sophisticated criminals, it can be used to make scams more elaborate and convincing.

The reality is that IoT is a “double-edged sword”. Indeed, having an IoT security cam that lets you see what is happening in your house via your smartphone might make a lot of sense when you are away but it also means that cyber criminals could watch you in your own home if the system had been compromised. Likewise, owning a smart TV that is voice-activated might seem like a nifty idea except that your privacy would vanish if hackers were able to listen in on your private conversations.

Common sense tells us that we should never share anything online that we do not want others to know about. But with the advent of IoT, the datafication of our most intimate personal information is unavoidable; more importantly, we will not have a choice about it. So if you are concerned about your online data privacy, then you should definitely be very worried about IoT.

It's Not All Bad – And besides Do We have a Choice?

Shunning IoT products completely would be unrealistic since they do bring important benefits. Furthermore, as existing electronic products get phased out, users have no choice but to replace them with IoT ones. Try buying a rear-projection TV today or apply for a job without a smartphone and you

will see the impracticality of snubbing the latest technology. If turning our backs on IoT products is not feasible, then what we need is prepare for its inevitable arrival.

For major organisations, this would mean integrating IoT products in a step-by-step fashion – taking the time to evaluate the technology with great care. The government can certainly help by assessing every IoT product for potential risks. If an IoT product is deemed too much of a cybersecurity risk then it should definitely not be integrated into a broader network.

The government also needs to set industry standards to ensure that IoT product manufacturers do not cut corners on their products since building in added security features will eat into their bottom-line. Apart from tightening security in the cyber domain, the government also needs to put tough data protection measures in place to limit abuses of personal information collected by IoT products. Lastly, consumers play a crucial role too; besides ensuring that their IoT products are secure, they must also be responsible enough to avoid those that are not.

When all is said and done, we need to recognise that at the moment no software-based product is really “hacker proof” and sooner or later, some IoT products will be breached by hackers. So some loss of online data privacy is to be expected as we enter the IoT age. The key then is finding that balance between risks and rewards – that sweet spot which allows us to enjoy the upside while keeping the pitfalls to a level that is tolerable.

REBALANCING ENCRYPTED MESSAGING APPS

This article first appeared in RSIS commentary

*Authored by
Tan Teck Boon*

Synopsis

End-to-end encryption has made instant messages more secure. But the technology has also made it more difficult for authorities to fight terrorism and crime. Reverting to the previous encryption technology rebalances security requirements with privacy concerns.

Commentary

THE RECENT decision by Brazilian authorities to ban WhatsApp – an instant messaging app used by millions of people worldwide – is emblematic of the kind of push around the world to rein in commercial messaging apps featuring state-of-the-art encryption.

In the case of WhatsApp, every message sent is encrypted with a unique “key” – typically, a very large number – ensuring that only the person(s) holding the specific key can unscramble the message. Even if a message were intercepted during transmission, it would be unreadable without the key. Besides WhatsApp, iMessage, Line, Signal and Telegram are some examples of commercial messaging apps featuring this technology.

To be precise, this form of encryption is called end-to-end encryption (or E2EE, for short). In earlier versions of the technology, the app developer retained the keys, thus making it possible for the developer to unscramble users’ encrypted messages under court orders. But with E2EE, the keys are kept in the users’ computer or mobile device and as a result, app developers are no longer able to hand over users’ encrypted messages even if ordered to. The only way authorities can gain access to users’ unscrambled messages in this case is to get physical access to their devices.

Upsetting Balance between Privacy and Security

History-wise, developers began seeing the need for more secure communications after a series of embarrassing photo leaks in 2014 involving quite a few female celebrities. But to be sure, monetary reward was also a big driver behind the development of encrypted messaging apps since the company that develops the app with the strongest encryption will invariably corner the lion’s share of this incredibly lucrative market. The advent of encrypted messaging apps would not have been a problem except that as instant messages became more secure, criminals and militants have also caught on to their usefulness – paradoxically exploiting for their own benefit the very justification that underpinned these apps in the first place.

Indeed, Islamic State (IS) militants are known to take advantage of these apps for secure communication as well as to reach out to potential recruits around the world. As a case in point, Malaysian authorities arrested three of its own citizens earlier this year who were thought to have been recruited by IS through Telegram. IS operatives also claimed responsibility for the recent Jakarta attack using the same messaging app.

But terrorists are not the only ones exploiting encrypted messaging apps; cyber-criminals, organised crime, drug dealers and even child predators use them to mask their illegal activities. Besides making it more difficult to monitor suspects, encrypted messaging apps have also made it harder for law-enforcement agencies to collect evidence against them. If anything, the situation now is akin to the police not being able to enter a house to collect evidence even with court authorisation.

Because encrypted messaging apps have made it significantly more challenging for authorities to disrupt terrorist plots and fight crime, the vital balance between privacy and security has arguably shifted in favour of the former.

Old Way Still the Best Way

One way to restore the current imbalance is to introduce so-called backdoors or hidden flaws into the apps so that authorities might gain access to the plaintext (unencrypted) messages of suspects. The backdoors could be introduced into either the hardware or software granting the authorities unlimited access. But even this strategy is imperfect. Apart from potential abuses, this approach can be downright dangerous since cyber-criminals and hostile foreign governments can exploit these built-in flaws just as well. Once a flaw is intentionally introduced into the system, it is only fair to assume that someone out there would find a way to exploit it for malicious reasons.

Technological advancement occurs at such a brisk pace that it sometimes blinds us to the fact that earlier inventions already held the solution to an existing problem. Indeed, by reverting to the previous encryption technology (in which the keys are retained by the app developer), the authorities can again monitor encrypted instant messages if needed. As in the past, app developer will act as a check against illegal government surveillance by scrutinising requests from the authorities for plaintext messages. The most obvious advantage is that authorities will right away regain the ability to monitor suspected militants' encrypted messages.

But what is less obvious is that reverting to the previous encryption technology will also serve to push them offline. In the same way Osama bin Laden promptly stopped using his Inmarsat satellite phone when the Al Qaeda

leader learnt that it was being monitored by US intelligence, the idea here will likewise push militants offline once they realise that the digital realm is no longer a safe haven from which to promote violence.

Unlike backdoors, reverting to the previous encryption technology will not lead to a spike in cyber-attacks because the previous encryption technology is sufficiently robust against the majority of cyber criminals. We know this because the authorities had to turn to the app developers for help and if they could not break into the previous encryption technology, then chances are run-of-the-mill hackers would not be able to either. Not all developers are expected to cooperate even though their apps now arguably threaten public safety and interest. But even if some were to, it will reduce the multitude of encrypted messaging apps at the moment and allow authorities to then concentrate their cryptanalytic effort on those that remain unbreakable.

Trump Card: Changing Attitudes toward Privacy

Reverting to the previous encryption technology will entail some risks to privacy. But it is still far superior and more realistic compared to introducing backdoors into every mobile device, computer and encrypted instant messaging software out there.

More importantly, our readiness today to share much personal information online in exchange for greater convenience and accessibility is indicative of our changing attitude towards the notion of absolute privacy. If anything, the popularity of cloud storage and social media websites these days really speaks to this shift in mindset. And as militants and criminals of all stripes continue to exploit encrypted messaging apps, reverting to the previous encryption technology will restore the delicate balance between privacy and security.



FUTURE OF POLICING IN GLOBAL CITIES

Prevention – Getting smarter, faster and more precise. Preparing strategies, approach and tactics for securing urban centers and global cities of the future.

The wave of digital technologies today is compressing the reaction time of police all over the world. It has set the stage for technologies such as social media, analytics and mobile to become game-changing forces for policing in the future. While technology alone is not the answer, there is now a growing consensus that technology transformation must be part of the overall solution. To keep our cities and citizens safe, law enforcement must be armed with the right technology tools as well as the right processes, behaviour and culture to solve – or even prevent – the toughest crimes at faster rates.

By 2020, the urban population is set to increase to more than 70% of the world's population. Driven by the need to stay connected, the ever-flowing transfusion of data and information can be the lifeline that keep cities safe, as long as threats are detected quick enough so that safeguards are in place, and counter measures are robust.

As the world urbanises, and cities move towards a “Smart City” vision, enabled by big data, network of sensors and the Internet of Things (IOTs), the magnitude of security risks and their frequency will inevitably change as will the nature of policing.

Digital technologies are already changing response time, crime prevention and investigations, and will continue to be a game-changing force for policing in the future. How police better coordinate, command and control critical resources and make quick sense of an explosion of information in crisis situations and emergencies is therefore critical in this regard.



Greg Basich
Senior Analyst
Automotive Multimedia and
Communications service (AMCS)

Greg Basich, Senior Analyst, Automotive Multimedia and Communications service (AMCS), has more than 13 years of experience in the automotive industry as a business-to-business online and print journalist and editor. He has covered a range of segments in the industry, including automotive infotainment and audio, fleet management, alternative-fuel vehicles and related technologies, and aftermarket parts and suppliers.

As an online journalist and editor, Greg stayed at the forefront of auto industry business news and technological developments and now uses that background at Strategy Analytics to provide analysis and actionable advice for the company's clients.

Prior to his time at Strategy Analytics, Greg was the Web Editor for Automotive Fleet and Government Fleet magazines for more than two years, and prior to that was the Executive Editor for Mobile Electronics magazine for two years, which focused on the U.S. automotive infotainment segment. He also worked in senior editorial roles on a number of other publications covering various segments of the automotive aftermarket.

Greg holds a BA in Economics from the University of California, San Diego.



Roger C. Lanctot
Director, Automotive Connected
Mobility
Strategy Analytics (AMCS)

Roger Lanctot has 25+ years of experience as a journalist, analyst and consultant advising electronics companies, car companies, wireless carriers, Tier 1s and developers on product and market development and strategy. Currently Director, Automotive Connected Mobility, in the Global Automotive Practice at Strategy Analytics, Roger is a thought leader on connected car technology. He is a graduate of Dartmouth College and a frequent blogger and keynote speaker.

THE STATE OF CYBERSECURITY IN THE AUTO INDUSTRY

*Authored by
Greg Basich and Roger C. Lanctot*

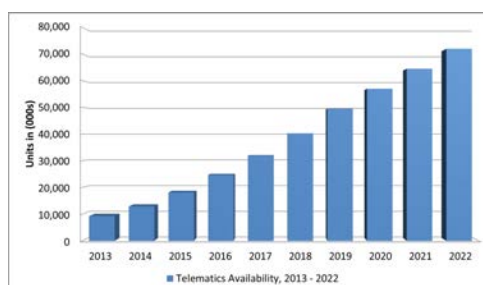
In the broader corporate world, businesses globally faced nearly 43 million security incidents in 2014, which is an increase of 48% over 2013 and equalling some 117 thousand incoming attacks daily, according to PwC's Global State of Information Security Survey 2015. That same survey pointed out a dramatic increase, 458%, in vulnerability scans (where hackers attempt to find security vulnerabilities) against devices considered part of the Internet of Things.

In addition to facing a digital environment experiencing more and more frequent attacks, automakers are embedding modems in vehicles at a faster rate than in years past, with millions of connected vehicles slated to reach the market this year and beyond.

For example, automakers deploying embedded modems that have not done so (or have done on a limited basis) in the recent past include Ford, with SYNC Connect Services, which launched in the 2017 Escape; Subaru, which added embedded modems to 95% of its models sold (by sales volume) in the U.S. this year under its (previously smartphone integration only) connectivity brand Starlink; and Nissan, which has launched Nissan Connect Services, starting with the 2016 model-year Maxima. In Europe, the upcoming eCall mandate will mean that all type-approved vehicles sold in Europe after March 31, 2018, will have embedded modems, dramatically increasing the number of vehicles with wireless connections that must be secured.

The following exhibit shows the number of vehicles shipped with embedded modems between 2013 and 2022.

Exhibit 1-1 Global Telematics Availability, 2013 – 2022, Per Year (Not Cumulative)



Source: Strategy Analytics

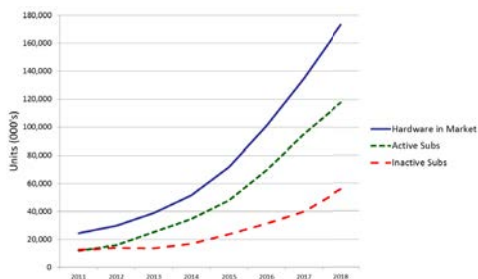
In light of these statistics, and the aforementioned hacks and related publication and publicity of those hacks, the auto industry is ramping up its efforts to protect its vehicles. This doesn't mean the industry is necessarily prepared to deal with any and all cyber threats — on the contrary, automotive OEMs have varying levels of security expertise and approaches to security. Up until the last few years, cars (and many still are) have not had as many wireless attack surfaces as they do today and therefore have had fewer security measures in place.

In addition, largely due to the long-term nature of the automotive design and production cycle, the hardware and software going into infotainment and other vehicle systems have already been built and designed, and in many cases contain vulnerabilities. OEMs have generally not designed vehicles to receive regular firmware or software updates, with updates largely confined to recalls performed by dealerships.

For example, many automotive infotainment operating systems are not updated after a vehicle is sold or, at best, go very long periods between updates. When the hardware and software in a vehicle were spec'ed, implemented, and locked down 2 to 3 years before the vehicle went into production (the average concept to deployment time for a vehicle in the auto industry is 39 months), any flaws that have been discovered since then may not necessarily have been fixed. In terms of fixing these vulnerabilities, enabling over-the-air updates have been proposed as the solution by numerous industry experts and security professionals.

This is definitely the path forward for future models, but for today's fleet this is simply not possible. Although many OEMs are equipping their vehicles with cellular modems, they are not prevalent and in many cases have been disabled due to the OEM's requirement to have a subscription to keep the modem activated.

Exhibit 1-2 Embedded Modems in Vehicles in Market vs. Inactive Subscriptions, 2011 – 2018



Source: Strategy Analytics

In some cases reactivation is possible, whereas in others it is not possible. In addition, many OEMs have not fully enabled over-the-air-update capabilities (OTA), despite having two-way wireless connections to their vehicles. In the FCA hack, for example, as noted

previously, the OEM mailed USB memory sticks to its customers to fix the vulnerabilities or asked customers to bring their vehicles to dealerships. Some OEMs have enabled over-the-air updates of various in-vehicle features, such as BMW (enabling OTA map updates), Mercedes (telematics features), and General Motors. GM's Phil Abrams has also gone on the record in an interview in the online media outlet The Verge, stating that the automaker has in fact rolled out various OTA updates over the years via the company's OnStar telematics platform, though he did not provide details about whether the OEM has delivered OTA updates beyond the TCU.

There are OEMs that have done more than simply update the headunit or TCU, but they are few in number. Tesla is notable for its ability to update multiple vehicle ECUs whereas for most other OEMs, OTA updates are confined to the infotainment system (headunit and/or telematics control unit). Even if others are capable of delivering OTA updates, many are wary of angering their dealerships (and inviting potential litigation) as they tend to view anything that would eliminate an opportunity for a customer to visit their service bay as a threat.

Beyond limited OTA updating capabilities, those employed in the industry are somewhat pessimistic about the ability to secure vehicles in the first place. Industry professionals also have questions about how (or whether) to replace vulnerable in-vehicle hardware and how long automakers should be responsible for maintaining in-vehicle software. For example, can an OEM declare a 15-year-old vehicle "obsolete" if its hardware and/or software could cause a life-threatening situation?

In one example of the auto industry's opinions on this subject, the Ponemon Institute, an organization that does research on privacy, data protection, and information security

policy, conducted a survey of 500 developers, 80% of which work for auto industry Tier 1 suppliers and OEMs, in cooperation with two companies, Security Innovation and Rogue Wave Software. The findings are cause for concern in the industry, to say the least.

Of those surveyed, 72% of developers said that the auto industry is less knowledgeable about secure software development than other industries. Less than half (41%) said secure software development was a priority for the company they work for, with 28% saying it was not a priority and 31% providing an “other” response, reflecting that they are unsure whether the company they work for takes security seriously. Also, 69% of those surveyed by the Ponemon Institute agreed that “securing the applications needed is either difficult or very difficult,” implying a lack of necessary knowledge and training. Nearly half of those surveyed (48%) said a complete overhaul of a car’s architecture would be required to make it more secure.

Beyond these issues, the majority of OEMs do not have clear guidelines or programs for working with outside developers who discover security vulnerabilities. For example, one of the few OEMs with a public “bug bounty” program is Tesla Motors. According to security experts who interact with automotive OEMs, it is often unclear which group or individual within a given OEM is responsible for dealing with bugs discovered by hackers, and in some cases OEMs are actively hostile toward white or “grey” hat hackers who report problems.

When it comes to software vulnerabilities that can be shared anonymously on the Internet and then exploited, trying to prevent that information from ever leaking is a losing strategy, so it is a better practice for the OEM to put in place a clear way to contact those working at the automaker who are responsible for security so that the vulnerability can be

brought to the company’s attention and (hopefully) fixed.

Despite the growing threats to vehicle cyber security, a common debate in the auto industry has been over whether vehicles actually represent attractive targets for hacking. The number of hacks that have occurred, including remote attacks such as the FCA hack, and the theft of BMW vehicles in the UK via low-cost devices, should end any debates about whether a vehicle represents a single, low-value target or not.

Vehicles today represent targets for the following reasons:

- **Vehicle and/or cargo theft:** Cyber criminals could gain physical access (e.g. unlocking a vehicle’s doors, trunk, or cargo area) to vehicles via wireless or wired connections to either steal the vehicle or its cargo
- **“Ransom” attacks:** Malware could disable a vehicle so it could not be driven unless the owner pays a fee to a criminal organization. This type of attack could also affect multiple vehicles, for example, crippling a company’s entire fleet until a ransom is paid.
- **Theft of Personal and/or Financial Data:** Data stored either in a vehicle’s ECU (e.g. the infotainment system) or on a server that the vehicle connects to can be a target for cyber criminals.
- **Property Damage and/or Injury:** Cyber criminals could simply be interested in causing mayhem, causing vehicle systems to fail while the vehicle is moving. If multiple vehicles within a fleet are affected, this could cause widespread loss of life, injury, and property damage, not to mention the liability an automaker would be exposed to in such a situation.

- **Industrial Espionage:** This would involve compromising vehicle systems to gain a competitive advantage.
- **“Hacktivism” or Terrorism:** Vehicles, especially those connected to wireless networks, could be used to cause injury and property damage. In addition, in the future as vehicles incorporate V2V, V2I, and ADAS and semi-autonomous features, they become more attractive targets as they could be used to cause mayhem, even if via relatively unsophisticated methods (e.g. spoofing sensor data to cause ADAS systems to activate and cause an accident, for example, stopping abruptly on the highway when there isn’t actually an obstacle present and causing multiple crashes as a result). Researchers have shown it is possible to spoof LIDAR sensor input via a laser pointer, for example.
- **Denial of Service:** Denial of service involves flooding a network with enough traffic to make it crash and become unresponsive.
- **Buffer Overflows:** This type of attack involves overwriting sections in memory that have defined sizes, causing systems to crash.
- **Fuzzing:** This type of attack involves inputting large amounts of malformed/random data (i.e. “fuzz”) in software applications, operating systems, and networks in order to crash it and thereby discover bugs and security holes.
- **Malware:** Trojans, worms, and other types of malicious software viruses can be used to enable control of vehicle functions and access to vehicle data, including any vehicle owner or passenger data that might be either stored in the vehicle (e.g. address destinations in a navigation system) or communicated via the network.

One of the major challenges automakers face is enabling delivery of over-the-air updates for the simple reason that patching software via USB (or other DIY method that involves the vehicle owner), or even at the dealer, is a losing proposition because not all vehicles will receive a given update via those methods. Even worse, criminals could distribute malware via USB by mailing vehicle owners USB drives with malware installed while pretending that the drive is from the OEM. The more serious the software issue is, whether hackers are exploiting it or not, OEMs are required to fix the problems or face a potentially costly recall.

1.1 Overview of Attacks

1.1.1 General Cyber Attack Examples

There is a wide range of attack types that malicious actors could employ and could apply to vehicles, depending on the automotive system being attacked. Examples of attack types include the following:

- **Replay Attack:** This is a form of attack on a network where a valid message/ transmission of data is repeated or delayed by a malicious actor with the intent to cause harm.
- **Side Channel Attack:** This is a type of attack that involves analysis of the physical characteristics of a given cryptosystem implementation. One example is differential power analysis, which involves analyzing the power consumption of a device when performing cryptographic computations in order to derive encryption keys. Another would be a timing attack, which would measure the amount of time a given computation takes in order to determine an encryption key.
- **Spoofing Attack:** A spoofing attack is where one device/system attempts to

impersonate another and send false/malicious information. One example in the auto industry would be a GPS spoofing attack, where false coordinates are sent to a vehicle’s built-in GPS receiver.

The attack types listed above are just categories that more specific types of attacks on automotive systems could fall into. For example, a malware attack could involve loading malware onto a smartphone and then when the smartphone’s owner connects that device to a vehicle’s infotainment unit, the owner unwittingly enables the malware to infect the vehicle’s headunit. The following section describes attacks on specific automotive systems in more detail.

1.1.2 Automotive Cyber Attacks

Cyber-attacks on vehicles have a few common elements. As has been described by a number of cyber security researchers focusing on the auto industry, the most dangerous types of attacks involve three stages, comprising an ECU via attack surface (remote or physical), sending messages from the compromised ECU to cyber physical systems in the vehicle (computational systems that control the physical actions the vehicle can take), which in turn instruct those cyber physical systems (e.g. ECUs controlling the brakes, vehicle speed, etc.) to take actions not intended by the operator of the vehicle. These types of attacks could cause accidents while a vehicle is in motion, unlock a vehicle’s doors to make it easier to steal, or make a vehicle inaccessible to the vehicle’s owner, for example.

Beyond compromising cyber physical systems, other attacks on connected cars could involve the retrieval of any stored personal information or eavesdropping on communications between the vehicle and external networks.

Exhibit 1-3 Attack Surfaces

Physical Attack Surfaces		
Automotive Attack Surface	Range	Threat Size
CD/DVD Drive	Physical Access	Single Vehicle
USB	Physical Access	Single Vehicle
Flash/SD Card	Physical Access	Single Vehicle
OBDII	Physical Access*	Single Vehicle
Remote Attack Surfaces		
Automotive Attack Surface	Range	Threat Size
Bluetooth	~10	Single Vehicle
Cellular	~8 to 75 km (depends on coverage)	Vehicles On Network
Dedicated Short Range Communication	~100 to 1000m	Vehicles In Range (viral)
Electric Charging System	~5-20m	Single Vehicle
Electronic Tolling (RFID)	~5-20m	Single Vehicle
GPS	~150m to 8 km	Single Vehicle
Near Field Communication	~20 cm	Single Vehicle
Passive Anti-Theft System	~10m	Single Vehicle
Radio (RDS)	~100m	Single Vehicle
Remote Keyless Entry (RFID)	~5-20m	Single Vehicle
Satellite Radio	~100m	Single Vehicle
Tire Pressure Monitoring System	~1m	Single Vehicle
Wi-Fi	~15m/Varies	Vehicles On Network

*OBD II dongles could potentially have wireless attack surfaces (e.g. Bluetooth, Wi-Fi, or cellular) and make the OBDII port more vulnerable.

Source: Strategy Analytics

Today’s vehicles are vulnerable due to the number of wired and wireless connections they present. Although technically everything from a CD to a car’s TPMS system can be hacked, connected cars without adequate security measures represent substantially easier targets for criminals.

- Bluetooth:** The Bluetooth stack is common in many vehicles sold globally, largely used to enable hands-free communication via tethered mobile phone. Researchers from the University of California at San Diego and the University of Washington found vulnerabilities in the Bluetooth software stack and determined that a paired Bluetooth device, for example via Trojan malware loaded onto the paired device, could enable execution of arbitrary code on the target ECU and on other ECUs on the network if the target ECU (e.g. the headunit) is not sufficiently separated from other networks in the vehicle.
- Cellular modem:** Cars with embedded cellular modems represent not only an attack surface that provides access to a given vehicle but also potential access to servers and other vehicles on the network that the

vehicle connects to. This is how Miller and Valasek (formerly of IOActive) were able to gain access to the CAN in-vehicle network on the Jeep they hacked. Miller and Valasek discovered they could scan Sprint's network for vulnerable Uconnect headunits (after scanning for open ports on the Wi-Fi hotspot gateway) and from there exploit the message bus system, which is the software that allows applications to talk to one another (in this case D-Bus). Miller and Valasek were theoretically able to affect any vehicle on the network prior to Sprint and Chrysler fixing the vulnerability.

- **Wi-Fi:** Vehicles with Wi-Fi hotspots, more common than ever before today (e.g. on Audi, BMW, Fiat-Chrysler, and General Motors vehicles, among others) present another wireless attack surface. For example, the network password could be compromised if its password generation method could only create a limited set of password possibilities. As researchers have demonstrated, although in many cases Wi-Fi is protected via some kind of encryption (e.g. WPA2, Wi-Fi Protected Access 2) and requires a password, depending on how the password is generated, it is possible to brute-force the password if it is not sufficiently difficult to do so. Beyond brute-forcing the password, if a device that has already been compromised is connected to the hotspot (a connected smartphone or tablet that an attacker has gained access to), then there is no need to bypass the hotspot's security because the device would have access to the network.
- **Brought-in device:** The majority of OEMs have enabled smartphone integration solutions of some kind, where the device can connect via USB, Bluetooth, or Wi-Fi. Since a user's mobile device can be infected with malware or otherwise compromised, as noted previously, there is a possibility for

attackers to gain access to the vehicle via the device.

- **OBD II Port:** The OBD II port is especially vulnerable due to it being relatively insecure and commonly used not only for its originally intended diagnostic purposes but also for new types of aftermarket telematics devices ranging from OBD II devices with built-in cellular modems to those that connect to smartphones via Bluetooth. This type of hack was demonstrated by a group of researchers. They were able to compromise the device (the researchers' paper, *Fast and Vulnerable: A Story of Telematic Failures*, goes into the technical details of their approach) and remotely use it to send CAN messages (via the OBD II port) to the vehicle network in order to take control of vehicle systems, such as windshield wipers and brakes. In the case of BMW, Audi, and other OEMs in Europe, criminals were able to retrieve keyfob codes from OBD II ports in victims' vehicles (after breaking into the car physically or jamming the transmission from the keyfob to the in-vehicle transponder) and copy them onto blank keyfobs in order to steal the vehicles.
- **Remote Keyless Entry (RKE):** Remote keyless entry systems can be (and have been) compromised via inexpensive hardware (the New York Times article *Keeping Your Car Safe from Electronic Thieves* cites a number of examples, e.g. brute-forcing a password or using a power amplifier in the proximity of the actual keyfob), for example to unlock a vehicle and make it, or its cargo, easier to steal. In general, the automakers encrypt communications between the keyfob and the in-vehicle transponder. OEMs generally use a challenge-response mechanism — the keyfob sends a request to the vehicle, the vehicle issues a "challenge," then the keyfob must respond with the correct response (i.e. the

password) to the challenge. In other cases automakers use rolling code (generated via pseudo-random number) generation to keyfob are able to communicate securely. Unfortunately, various techniques, from jamming (to prevent someone from locking their vehicle) to power amplification in proximity to the actual keyfob have enabled researchers and criminals to bypass remote keyless entry security systems.

- **Tire Pressure Monitoring System (TPMS):** TPMS systems are not necessarily connected to a given vehicle's network but researchers have demonstrated the ability to hack TPMS sensors to either cause the sensor's companion ECU to malfunction or to track the vehicle.
- **Vehicle-to-vehicle communications:** The current proposed method for vehicle-to-vehicle communications, Dedicated Short Range Communication (DSRC), presents yet another attack surface and cyber security challenge. The combination of large numbers of vehicles constantly communicating with each other, as well as the related location data for the millions of cars on roads in regions of the world, all contributes to a mix of networked attack surfaces that could rapidly enable the spread of malicious code capable of causing widespread damage unless those communications are secured. The IEEE has provided for security in its specification, with IEEE 1609.2 specifically dedicated to the implementation of security when using DSRC for V2V communication. In Europe, the European Telecommunications Standards Institute (ETSI) provides the TS 103 097 standard for V2V communication.
- **Electric vehicle charging stations:** Modern EVs communicate wirelessly with electric vehicle charging infrastructure. Charging stations often use inexpensive RFID cards

without encryption. Physical access to these stations is generally simple, often a panel secured with a lock. Hackers can physically break into a charging station to get access to components. They could also connect via processor ports to get access. Potential attacks could involve eavesdropping on wireless communication, for example to steal vehicle owner data (e.g. identity, financial transaction information, etc.) or cause damage.

1.2 Types of Security

Securing modern vehicles involves a number of separate layers, each of which is designed to prevent one of two things from happening:

1-Loss of control of vehicle functions

2-The exposure of information that could be used to the detriment of the vehicle owner, automaker, or other automotive product or service providers

With this in mind, there are a number of approaches to securing vehicle systems that can be applied to a range of systems in the vehicle. This section will cover each of them broadly and then go into more depth with respect to specific automotive systems. As always, there are pros and cons to each approach in terms of processing overhead, complexity, dealing with conflicting priorities (in some cases security vs. safety or privacy), and cost that OEMs and suppliers must consider.

Security generally falls into three categories, hardware-enabled, software-enabled, and security services. Examples of each include the following:

Hardware-Enabled Security

- Gateway Module
- Tamper-proofing
- Side-Channel Attack Protection
- On-Chip Device Identity

- Cryptographic Acceleration
- Secure Boot
- Memory Protection
- Domain Isolation
- Secure Key Storage
- Secure Debugging

Software-Enabled Security

- Firewalls
- Network Behavior Enforcement (e.g. restriction of which ECUs can communicate, message volume restrictions)
- Authentication
- Encryption
- Intrusion Detection and Protection
- Whitelists/Blacklists
- Application Sandboxing
- Virtualization

OTA and Security Services

- Over-the-Air Updates
- Public Key Infrastructure/Digital Certificate System Support
- Security Consulting
- Penetration Testing

With this list in mind, upcoming sections will cover each of these methods in greater depth.

1.2.1 Hardware Security

Hardware security can be enabled at the semiconductor level, with many semiconductor companies providing automotive grade microcontrollers that come with a number of security features. Those types of features include the following:

- **Tamper Resistance:** Tamper resistance involves a number of methods for preventing access to the device, such as using sensors to detect tampering (light, resistivity, or temperature sensors), deleting cryptographic keys when a physical breach is detected, hardened casings (for preventing physical access), and the use of error-correcting memory.
- **Side-Channel Protection:** Side-channel attacks can be mitigated by adding randomness to, or reducing leakage of, information that could be obtained via a side channel. Examples of protection include adding random delays to prevent timing-based side-channel attacks; reducing electromagnetic leakage from a device; and modifying cryptographic protocols to reduce how much information an attacker could obtain from a side-channel attack.
- **Unique Device ID:** Each ECU on the network has a unique identity, stored on the device, which ensures that the manufacturer knows the identity of each device and prevents devices without known/approved identities from accessing vehicle networks and related systems.
- **Cryptographic Acceleration:** Cryptographic algorithms require processing power and providing a dedicated co-processor to handle encryption-related tasks can free up the host processor for other uses (e.g. infotainment-related processing).
- **Secure Bootloader:** The ECU in question checks the boot loader's digital signature and product keys, as well as the signatures of other operating system files, to ensure those components have not been modified. If the system detects any files that are invalid, they are prevented from operating.
- **Memory Protection:** Buffer overflows/overruns, integer overflows, null pointer references, and other types of memory corruption problems can be caused by attackers when code is not written to protect against these types of issues. Actively protecting memory can involve a range of methods, from canary values (a randomly generated integer located before the return pointer on the stack that is checked prior to a routine using the return pointer), bounds

checking (checking pointers against each block of memory's size before use to ensure it can't be overwritten), and tagging, which involves marking blocks of memory such that they can't contain executable code.

- **Domain Isolation:** ARM and other semiconductor companies provide support for domain isolation in silicon. One example is ARM's TrustZone solution, which enable a single processor to run code from two different "domains," the "Normal" domain and the "Secure" domain, separating functionality. One common approach is to use a gateway module to coordinate the flow of data between different vehicle domains. The gateway can transmit data between the data bus for systems in the engine compartment, the interior bus, the infotainment bus, and the diagnostic bus. The key security feature, of course, is physical separation of domains and the ability to enable various types of security software on the gateway to monitor and control the data that reaches different vehicle systems.
- **Secure Key Storage:** This involves storing encryption keys in non-volatile memory in order to prevent them from being exploited.
- **Secure Debugging:** Debugging interfaces in hardware should have some kind of security implemented in order to prevent unauthorized access to a debugging mode. At the very minimum, some kind of authentication (e.g. password protection) is essential. Secure debugging generally means that access to a debugging mode is locked by default and the device is not readable via the debug interface.

Currently, many suppliers provide a mix of these types of features in their solutions. In the semiconductor space, for example, at this time many provide features based on

variants of the Secure Hardware Extension (SHE) specification. The original specification came out of the European Union EVITA project (detailed below) and since then many companies have created other types of specifications to further develop the capabilities of hardware security modules. Different types of hardware security modules could be used with different types of ECUs in the vehicle, depending on the nature of the attack surface. Another type of hardware security specification is the Trusted Platform Module, which is covered below as well.

1.2.2 Hardware Security Specifications EVITA

EVITA (E-safety vehicle intrusion protected applications) was a European Union project to design and prototype a type of vehicle network architecture to ensure the security of vehicle systems. One of the primary results of this program was creation of specifications for variants of what the project called a "hardware security module," abbreviated as HSM, a hardware-based approach to securing in-vehicle networks.

EVITA partners included BMW, Bosch, Continental, Escrypt (now a Bosch subsidiary), Eurecom, Fraunhofer, Fujitsu, Infineon, University of Leuven, MIRA, Telecom ParisTech, and Trialog.

The program produced three different specifications, HSM Light, also known as a Secure Hardware Extension module (SHE module), HSM Medium, one example of which is Tier supplier Bosch's HSM, and HSM Full, which provides hardware-based features for securing V2X communication channels in addition to the vehicle network. The SHE specification is designed to be integrated into semiconductor solutions, whereas a full HSM is a separate hardware module.

The following chart depicts some of the major differences between the HSM types:

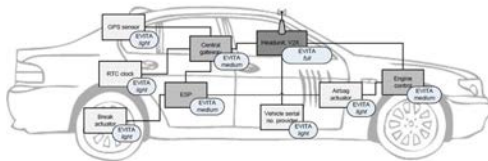
Exhibit 1-4 EVITA HSM Level Differences

EVITA HSM	EVITA Full	EVITA Medium	EVITA Light (Secure Hardware Extension)
Internal RAM	Yes	Yes	Optional
Internal Non-Volatile Memory	Yes	Yes	Optional
Symmetric Crypto Engine	Yes	Yes	Yes
Asymmetric Crypto Engine	Yes	No	No
Hash Engine	Yes	No	No
Random Number Generator	Yes	Yes	Optional
Secure CPU	Yes	Yes	Yes

Source: ERTS 2014 Conference Proceedings

A simple example of how different types of hardware security modules would be applied to the vehicle's ECUs is shown in the following diagram from an EVITA project presentation.

Exhibit 1-5 Hardware Security Module Deployment Example



Source: EVITA

In terms of forecasts, Strategy Analytics' Powertrain, Body, Chassis, Safety service sees approximately 88% of 2020 32-bit MCUs having some form of encryption. That said, by far the largest category (55%) would be EVITA Medium specification devices. Only approximately 5% of controllers are estimated to be "EVITA High," with highspeed hardware acceleration for hash, ECC, and AES.

1.2.3 Trusted Platform Mobile

Another approach to securing hardware being taken by various OEMs, such as Toyota, is the use of the Trusted Computing Group's Trusted Platform Module (TPM). The TPM is a specification for a cryptographic processor

on a chip that is designed to provide secure encryption key storage, non-volatile memory, and a random number generator. The TPM has been through various specifications — the latest version is 1.2 and 2.0 is in development. Encryption algorithms supported by version 2.0 include SHA-1, SHA-256, RSA, and Elliptic Curve Cryptography P256. Semiconductor suppliers, for example Infineon, provide a TPM for automotive use (Infineon's specific product is the OPTIGA TPM). There are pros and cons to the TPM, such as the additional cost of integrating an extra external chip inside a given ECU.

1.3 Software Security

1.3.1 Software Security Measures

The key to all automotive cybersecurity is taking a layered approach. These methods can be used to secure the hardware and software layers of vehicle systems. The following section provides an overview of different methods in the context of different hardware and software layers.

- **Firewalls:** Firewalls block unauthorized data packets from reaching their intended target, for example, a given ECU. In the automotive environment, firewalls could, for example, be used in a gateway processor to protect access to the different networks in the vehicle. Firewalls are also used to protect wireless interfaces from potentially harmful communications.
- **Intrusion Detection and Prevention:** Intrusion detection is implemented via a software security layer that monitors incoming communications (from wired or wireless sources) and in-vehicle network traffic, to identify and prevent abnormal data transmissions from affecting a vehicle's operation. Examples of ways an intrusion detection system could respond include blocking traffic from a malicious source,

resetting a connection to an outside source, and notifying another system or outside source that something is wrong.

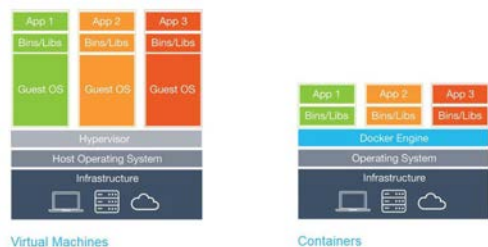
- **Authentication:** Authentication can be used to add a layer of security to any communication channel between a vehicle's systems and with systems and devices outside the car. Authentication, in this context, simply means that a message (command, data, request, etc.) being sent between systems comes from an identifiable source and that the recipient of the message is supposed to be receiving a message from that source. There are many ways to implement authentication, depending on the type of system being protected, such as message IDs and passwords.
- **Whitelist/Blacklist:** Whitelists and black lists are forms of authorization, which is a step beyond authentication. The sender must not only provide proof of identity but also proof of authorization to be sending messages in the first place, i.e. that the sender has the correct role, or access level, to do so. A whitelist describes which applications can run on a given OS or which messages can be sent by ECUs to the ECUs. A blacklist is similar to a whitelist but instead describes which applications (e.g. known malware) cannot run on a given OS. A blacklist could also block communications from specific sources.
- **Isolation:** Isolation is the separation of vehicle systems, either physically or at the firmware or software levels. As an example this could involve separating the infotainment and ADAS domains, since ADAS features often present a number of cyber physical features that if compromised could endanger vehicle occupants.
- **Virtualization:** Virtualization, either with type 1 (bare metal, where guest OSes run

on top of the hypervisor) or type 2 (the hypervisor runs in a host OS) hypervisors, virtualization enables multiple operating systems and applications to run on the same processor. There are disagreements over whether virtualization is sufficient to completely separate safety critical and infotainment/non-critical domains, but security experts generally agree that any separation of domains is better than no separation. With the industry moving toward the merging of safety critical and infotainment domains, for example for the purposes of providing advanced driver assistance system (ADAS) alerts to the driver, virtualization is a good option as it provides separation of domains.

Another form of virtualization is the container (a popular version in the Enterprise space is Docker, which is the name of the solution and the company supporting it), which is not inherently secure, but can be secured through various methods (e.g. Docker 1.8 provides what the company calls Docker Content Trust, a public key infrastructure approach, with a public "Tagging" key and a private "root" key).

The diagram below shows the fundamental difference, in this case using Docker as an example from the IT world, between a container and a more traditional type 2 hypervisor (with the hypervisor running in an OS rather than on bare metal) approach.

Exhibit 1-6 Virtualization vs. Container



Source: Docker

In the auto industry, Linux containers can be used to run Android on top of a host operating system. Mentor Graphics provides training content for this approach, including a section on securing Linux containers.

- **Network Behavior Enforcement:** This involves creating a model of normal vehicle operations, using software to look for abnormalities in those operations, and then enforcing those operations. This would include looking for malicious attempts to gain access to vehicle systems from the outside, monitoring messages on the vehicle network looking for abnormalities in terms of the number of messages sent in a given period of time or message content, and monitoring software applications to ensure that they are operating as expected. Behavior enforcement can take the form of restricting which ECUs are allowed to communicate with one another and restricting message volumes. Malicious messages on CAN, for example (as noted by Miller and Valasek in their published research while with IOActive) would be sent at a higher rate than normal. Detecting an abnormal number of messages being sent on CAN within a set period of time, for example to take some action to prevent the malicious messages from being acted on, is one example of enforcing expected network behavior.
- **Logging System:** Without a logging system (a log is generated by the system and is a record of user and system activity on the vehicle's network(s)), it is impossible for an OEM to conduct cyber forensics to determine when and how hackers or criminals hacked a vehicle (or vehicles). A system such as this should conform to the legal standards for cyber forensics, for example to ensure a chain of evidence.

Beyond simply having logs, there must be a system in place for capturing, storing, and analyzing log data. OEMs must also have a policy for managing those logs in the organization. In addition, it is a good idea to separate personnel duties to prevent concealment of anything illicit by employees. The logging system should also be designed with vehicle owner privacy in mind, for example to comply with regional laws and regulations regarding data storage.

1.3.2 Encryption

Encryption involves using cryptographic algorithms to make data unreadable except by the intended recipient of the data. Encryption can be symmetric or asymmetric. This section provides additional information about this topic as it applies to many other areas of security.

- **Symmetric Encryption:** Both the sender and recipient possess the key needed to encrypt and decrypt data sent by the sender to the recipient. The key must therefore be distributed securely to avoid it being compromised.
- **Asymmetric Encryption:** There are two keys, a public key and a private key. The public key can be used by anyone (i.e. any system or device) to encrypt a message (i.e. data), but only the intended recipient of the message has the private key that enables decryption of the message. Asymmetric encryption can also be used to enable the use of digital certificates. In that case, the sender would use a private key to “sign” a message and the receiver would use the corresponding public key to verify that the message was indeed from the sender. In practice, messages and software that use certificates are “signed” by a certificate authority, a third-party company/entity, that attests to the identity of a message or software program, for example the identity of the sender or software provider. A digital

certificate includes the identity of the sender and the public key from the public-private key pair.

Encryption can be used to secure communication between ECUs in the vehicle, i.e. messages sent over CAN, MOST, Ethernet, etc., and between vehicle ECUs and outside devices and systems, for example by connecting the headunit to a mobile device via Wi-Fi or a telematics control unit to a cellular network. Symmetric encryption has less processing overhead than asymmetric encryption.

There are a number of encryption algorithms that can be used, including RSA, ECC, AES, SHA, and DES, among others. In many cases semiconductor vendors' solutions support various types of encryption. These types have various uses. Select examples include the following:

- **Secure Hash Algorithm (SHA):** This is a family of hashing algorithms published by the U.S. National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing (FIPS) standard. There are a number of algorithms part of this family, including SHA-1 (which has been considered insecure since 2010), SHA-2 (a group of algorithms, SHA-256 and SHA-512, where SHA-256 uses 256-bit words and SHA-512 uses 64-bit words for encryption, though there are also shortened versions such as SHA-224, SHA-384, SHA-512/224, and SHA-512/256), and SHA-3 (it has the same hash lengths as SHA-2 encryption but a different design, and is now a new hashing standard, according to NIST, as of Aug. 5, 2015). SHA has been used for asymmetric encryption, for example for digital certificates used part of a public key infrastructure (PKI) system.

- **Advanced Encryption Standard (AES):**

This is a specification for symmetric encryption (in automotive usage, as noted previously, this could be used to encrypt communication between ECUs on a given vehicle network). Also as described previously, with symmetric encryption, the same key would be used to encrypt and decrypt data sent over the network. AES has a block size of 128 bits but variable key sizes, including 128, 192, and 256 bits.

- **True Random Number Generation (TRNG):**

This is a way of generating a true random number in hardware, via methods such as statistically random “noise” from various phenomena, for the purpose of generating new cryptographic keys. Many suppliers of semiconductors for embedded systems, including automotive usage, provide in-silicon TRNG.

- **RSA:**

RSA is an asymmetric “cryptosystem” where each letter stands for the name of one of the creators of the system. RSA encryption, since it’s used for asymmetric encryption, uses a public key for encryption and a separate private key for decryption. There are four stages used to secure data transmission when RSA is used: 1-generation of public and private encryption keys, distributing those keys to the correct/authorized parties, encryption data to be transmitted via the public key, and then decrypting received data via the private key held by an authorized recipient. Since RSA is used for asymmetric encryption, an automotive use case would be securely transmitting over-the-air updates to vehicles.

- **Elliptic Curve Cryptography (ECC):**

ECC is a methodology for public key (i.e. asymmetric) cryptography that makes use of the equation used to define elliptic curves over a fixed range of values (whole numbers over a finite range). ECC leads to encryption that is harder

to break, i.e. requires more computational power, for the same key size than RSA. The use of ECC (and other types of asymmetric cryptographic methods, such as RSA) comes with a caveat, though, that is explored later in this report, due to the emergence of quantum computing technologies.

The encryption scheme used must, of course, be supported by not only the semiconductors used in a given ECU but also by the in-vehicle network type itself. Standard CAN, for example, does not have the bandwidth to support strong symmetric encryption algorithms. Newer CAN standards, such as CAN-FD (which has bandwidth of between 2 and 4 Mbit/s and data length of up to 64 bytes), may be able to support some level of encryption, though even CAN FD does not have built-in security features.

In the near term, OEMs should be considering a move to Ethernet, which does have built-in security features (as detailed in this report), and is a better choice due to those features and the higher bandwidth it provides (not to mention the need for Ethernet when dealing with ADAS and autonomous driving features and systems, though that discussion is beyond the scope of this report).

With respect to some recent changes in guidelines for encryption types to use, Microsoft, Mozilla, and Google have all officially dropped support for SHA-1 certificates. In addition, Google broke the encryption algorithm (i.e. generated a collision, where Google was able to produce the same hash in two separate files) in February, 2017. The companies noted above will also no longer support the RC4 encryption algorithm when used with TLS or SSL.

The reason for the change is that it's become much more cost-effective to forge digital certificates that use SHA-1 encryption,

making them insecure. Beyond these near-term changes, another major technological advancement that will likely have a dramatic effect on encryption, assuming progress continues, is quantum computing.

1.4 In-vehicle Network Security

Securing the in-vehicle network, e.g. CAN, LIN, Flexray, MOST, and Ethernet, involves its own discussion since doing so is complex. Vehicle Architecture Decisions: In-vehicle communication networks provide different features out of the box, depending on whether an OEM is choosing CAN, LIN, Flexray, or Ethernet for different systems within a vehicle.

As vehicle networks have become more complex, approaching 100 separate ECUs with different functions and related firmware and software, and attack surface have proliferated. Thus far the types of vehicle networks commonly used in the auto industry haven't adapted well as many were simply not designed with security in mind.

Encrypting messages sent among ECUs on a vehicle network is one way to improve security. Researchers have suggested that symmetric encryption would be sufficient to ensure that messages on the vehicle's network aren't malicious. There are issues with implementing this type of security for CAN-based networks, however, due to the small message size and inherent limitations of CAN as a protocol.

1.4.1 Securing CAN?

CAN was developed by Bosch in the early 1980s and formally released in 1986. CAN is a broadcast-based protocol whereby an ECU on the network broadcasts its message to all other ECUs on the network and those ECUs choose whether to respond based on what is called the message's arbitration ID and subject. Only a single message exists on the network at a given time. CAN messages are automatically

triggered by events on the network. CAN also contains a provision for re-transmitting messages following error messages.

CAN messages consist of three major parts, typically an 11-bit arbitration ID (though extended versions of CAN provide message frames with IDs that are 29 bits in length), a data length code (4 bits in length), and generally up to 8 bytes of data (as noted previously, a CAN variant, CAN FD, provides up to 64 bytes of data).

The arbitration ID represents the message's subject and priority (the lower priority ID wins), and although could technically be used to identify the device that sent it, it does not actually contain data that identifies the sending ECU or the recipient ECU. For example, an ECU on the CAN network can send messages with different arbitration IDs.

Beyond the lack of true identification of the sending ECU and recipient, CAN messages also do not automatically include any kind of encryption. Although CAN messages do include an error checking method (e.g. a cyclic redundancy check, i.e. a checksum that determines whether the message was the correct length and therefore whether an ECU should accept or reject a given message), a malicious sender could "forge" the CRC, thereby bypassing it.

The point of bringing this topic up is to note some of the fundamental issues with a very common standard used for in-vehicle network communication in the auto industry.

CAN was designed for vehicles from a different era, when tampering with a vehicle required physical access and time. For OEMs and suppliers implementing variations of the CAN protocol in the future, securing this type of network requires putting in place types of security that can shore up CAN's inherent limitations.

1.4.2 LIN

LIN, which stands for Local Interconnect Network, is an inexpensive serial network protocol that enables components in a vehicle to communicate with one another. LIN is typically used to control relatively straightforward vehicle systems, such as light controls in a roof-mounted light, motors in a seat, power windows, or steering wheel functions (windshield wiper, turn signal, etc.).

LIN uses a master-slave method of controlling nodes on the network, with a single master node and a number of slave nodes, generally between 2 and 16. LIN is designed as a "sub-bus" system, where the master node would connect to the CAN bus. The master node determines the specific messages that can be transmitted on the bus and the timing of those messages. Bandwidth is up to 20Kb/s. LIN messaging is deterministic in nature rather than event-triggered and messages are delivered with guaranteed latency times.

With respect to security, the LIN protocol does not allow slave nodes to send messages unless the master node requests a response, but if the master node was somehow compromised, then all slave nodes connected to the master node would be compromised as well. The master node can also send messages to any other ECUs on the CAN bus since it is linked to the CAN bus.

1.4.3 FlexRay

FlexRay is an in-vehicle network protocol that makes use of both time-triggered and event-triggered messaging. It operates similar to CAN in that FlexRay has higher bandwidth than CAN, between 5 and 10 Mbits/second. FlexRay utilizes a master node that provides a message timing reference for all other nodes on the network. FlexRay also utilizes what is called a "bus guardian," which is used to handle errors. FlexRay has a 1ms communication cycle that consists of a static

segment, which is designed for real-time triggered events, a dynamic segment, that can be used for asynchronous triggered events, a symbol window (used for starting the network and network maintenance), and network idle time, which is used to keep the clocks of the nodes on the network synchronized.

According to research published by Escrypt conducted by Marko Wolf, André Weimerskirch, and Christof Paar, malicious error messages received by FlexRay's bus guardian could be used to deactivate other ECUs on the network. In addition, FlexRay does not contain any specific type of authentication nor is communication on the network necessarily encrypted.

1.4.4 Ethernet

Automotive Ethernet, still not widespread but beginning to appear in the auto industry (for example in BMW's X5), does include some basic security measures. In addition, it can benefit from security measures already in use in other industries that currently make use of Ethernet.

Auto industry professionals have varying opinions on whether improved security will require Ethernet. In the Ponemon Institute survey cited previously, 20% of respondents said they should replace current in-vehicle networks with automotive Ethernet. A total of 35% said it should be replaced, but with something other than Ethernet. Nearly 40% (39%) said Ethernet was not required, and 6% of respondents were unsure.

Some examples of the basic level of security built into Ethernet that are a packet format that includes addresses for the packet source and destination, a frame check to insure data integrity, and an optional VLAN (virtual LAN) tag.

One way of implementing greater Ethernet security would be to first organize the domains

on the network around separate VLANs and from there use VLAN tags in Ethernet messages to direct packets to a specific VLAN. Ethernet provides other security benefits over CAN and older network types. The 802.11 AE Mac Security standard provides for media access control-level encryption as well as message authentication when using Ethernet for the exchange of secure keys. Media access control is the lower level of the data link layer, the layer responsible for transferring data between nodes in a network, within the Open Systems Interconnection model, which is a model for how the communication functions for a computing or telecommunications system can operate. The 802.1X protocol provides for passing Extensible Authentication Protocol (EAP) frames over Ethernet, enabling authentication of messages.

One challenge is when the messages sent via an ECU are legitimate but potentially dangerous (e.g. activating the brakes, a normal type of vehicle operation, but in a situation where doing so would cause an accident), the implemented security solution must have some idea of the vehicle's "state," i.e. what constitutes normal operation of the vehicle. Without situational awareness, for example via sensors and related safety functionality, however, this is challenging to implement. The auto industry is moving in the direction of implementing "sensor fusion," which would allow for centralized processing of sensor input and therefore enable the vehicle to "know" its state. That said, the industry is not there yet and still has a long way to go before vehicles have this basic level of situational awareness.

1.5 Over-the-Air Updates and Security Services

1.5.1 Over-the-Air Updates and Cloud-Enabled Security

Cloud-enabled security involves providing

vehicle cyber security via cloud-based methods. Of course the servers and software running on those servers must be secured as well, but that topic is beyond the scope of this report. There are a number of methods for providing security via an off-board connection that can be implemented.

- **Secure Channel to Cloud Servers:** Any connection a vehicle makes with off-board servers should be secured.
- **Remote Monitoring of Vehicle Systems:** The two-way connection enabled via a cellular modem enables periodic wireless monitoring of a vehicle's systems.
- **Over-the-Air Updates:** Over-the-air updates are a common method prescribed today for updating software in vehicles. There are three security components to OTA updates:
 1. Delivering security patches/updates via over-the-air updates
 2. Securing the wireless channel by which OTA updates are delivered
 3. Securing OTA updates conducted at the dealership (insider attacks are a possibility in this case)

The majority of over-the-air update solutions in the market today involve an ECU in the vehicle, for example the headunit or TCU, with a software client of some kind that communicates with off-board servers and manages downloading and installation of updates.

Securing these updates requires a mix of authentication, validation, and encryption. When an update is available, the server delivering the update must notify the vehicle (via a push notification) that the update is ready. From there, the software client in the vehicle would authenticate the update and verify the version, then install it. Updates would be digitally signed via an off-board certificate

management system. Of course other vehicle systems must be secured in order to facilitate these updates. For example, the bootloader must verify that the update is in fact correct prior to booting up the ECU that was updated.

At this point in time OTA updates are generally confined to a small number of ECUs, for example the headunit or telematics control unit. Only Tesla, thus far, has demonstrated the ability to update firmware and software in a range of ECUs in the vehicle.

In many cases, ECUs used by OEMs are not necessarily updateable in the first place. Many OEMs are taking a conservative approach, intending to only allow updates of the headunit or telematics control unit. Although the intent may be to isolate domains, the convergence between ADAS, autonomous driving, and infotainment systems means this will be difficult (if not impossible) to achieve without some level of integration/communication between vehicle systems. As has been noted previously in this report, a range of security measures, including the ability to provide security updates, are essential to securing connected vehicles.

Based on conversations with companies providing OTA solutions in the marketplace, updating ECUs beyond the headunit or telematics control unit is unlikely to be widespread in the auto industry until the 2019-2020 timeframe despite a growing number of cars with embedded modems on the road between now and then.

1.5.2 Security Services

A critical part of a functional automotive cyber security program at an automaker or supplier is engaging with third-party cyber security experts. In this day and age it's generally not possible for most organizations to conduct all necessary security testing, and have enough employees with expertise in the right fields,

to evaluate, test, and implement security for vehicles and related subsystems.

- **Security Consulting:** Security consulting involves reviewing a number of areas with respect to cyber security, from an organization's security development and response processes to engineering reviews of vehicle architectures and systems. Automakers and suppliers should evaluate consultants based on both their level of automotive and embedded systems background as well as on specific areas of expertise that relate to connected cars, for example wireless security (cellular, Wi-Fi, Bluetooth, etc.).
- **Penetration Testing:** Penetration testing is a specific type of security consulting that involves hiring experts to attempt to compromise a given module, system, or vehicle in general. This is a type of testing that needs improvement in the auto industry, as pointed out by the industry professionals Strategy Analytics spoke with, is penetration testing of full vehicles rather than only specific systems, and testing that takes place much earlier in the vehicle development cycle rather than at the end of production.

1.5.3 Tesla Motors' Cyber Security Measures

Tesla Motors has been much more public about the cyber security precautions it takes with its vehicles. Tesla is also notable as it has quickly been able to address security issues that researchers have discovered through a combination of over-the-air updates and an in-vehicle network (Ethernet-based) with ECUs designed to be updated. An article in Automotive News highlighted the specific measures the OEM has put in place.

Tesla uses the following security measures:

- Filters, firewalls, and a design that does not require direct, incoming connections from the Internet
- Domain isolation via a physically separate gateway processor
- Use standard encrypted communication protocols for connections from the vehicle to outside devices/systems/networks
- Digital signatures to ensure that only Tesla authorized security is being installed and/or running on its vehicles

**Hong-Eng Koh**

Global Chief Public Safety Expert
Enterprise Business Group
Huawei Technologies Co., Ltd

As a thought leader in Public Safety and Justice (PSJ), Mr Koh is the chief expert in Huawei on the use of Information and Communication Technologies (ICT) in enabling and even differentiating PSJ agencies for a safer city and nation. He is a well sought after speaker internationally and is well regarded in evangelizing the “It takes a Network to Fight a Network” principle in countering crime, terrorism and disaster. Mr. Koh is also the creator of the “Social-Enabled Policing” concept: policing in the age of social networking and crowd-sourcing. Prior to joining Huawei for this pioneer global chief expert position, Mr. Koh spent more than 15 years in Oracle, including Sun Microsystems which was acquired by Oracle. He was the Global Lead in PSJ with similar roles as in Huawei.

Mr Koh started his career with the Singapore Police Force (SPF) after graduating under an SPF scholarship. He held various appointments including senior investigation officer, head of crime prevention and community policing, police spokesman, and divisional head of operations and training. His last appointment was as head of the Computer Systems Division, where he led the implementation of various police operational and administrative systems. During his years of service in SPF, he received various awards including the Commissioner’s Commendation and High Commendation, Good Service Medal, Long Service Medal, and Good Conduct Medal.

THE ROAD TO COLLABORATIVE PUBLIC SAFETY DIGITAL ECONOMY OR DIGITAL DISRUPTION?

*Authored by
Hong-Eng Koh*

We are already in the age of the digital economy. New technologies are facilitating greater connectivity between people and devices, enabling crowd-sourcing, increasing efficiencies of traditional processes, and even creating new business models such as Uber, Airbnb, Alibaba, Facebook, WeChat, and many others.

While these new business models are celebrating the Digital Economy, some traditional businesses (e.g., taxis, hotels and telcos) see this as Digital Disruption. The reality is that industries that are not already transforming themselves will soon be disrupted by digital technologies.

Unfortunately, our adversaries are also transforming themselves through the use of technologies driving this Digital Economy: Social, Mobile, Cloud, and Big Data! We see some extremist groups using such technologies to aggressively radicalize, recruit, seek finance, and even to collect intelligence. Criminals have also exploited digital technologies to carry out various crimes.

It is therefore imperative that we form a network of 'good guys' to fight against the network of 'bad guys'.

Safe Cities

According to IHS Technology, video surveillance, Long-Term Evolution (LTE), and command and control solutions are the backbone of a Safe City. The three key aims of these technologies are:

- To ensure reliable and all-coverage security measures to detect threats and situations as they emerge.
- To aid public safety organizations in collecting, sharing and analyzing data more effectively

to provide a common operational picture and raising situational awareness.

- To enable key entities of a city to identify and act in real-time to security threats of any scale.

With more than 200 Safe City projects in more than 40 countries serving more than 800 million people, Huawei's Safe City solutions are renowned globally. Real-time video communication in this day and age is imperative to public safety. Huawei provides such trunking capabilities from backend networking to devices supporting LTE, both public (LiTRA) and private (eLTE). The devices, ranging from handsets to in-vehicle terminals, support voice, data, and video. There is even the eLTE Rapid System, which integrates various components into a compact chassis ideal for rapid deployment in the field where there is limited data coverage such as a disaster site where key infrastructure has been crippled.

At the heart of Huawei's Safe City solutions is the Integrated Communications Platform. This platform supports interoperability of eLTE, and legacy TETRA and P25 devices. It can even connect to conventional telephone networks and cellular networks. In line with a visualized command center, this platform accepts videos from multiple sources. It is also ready for the Digital Economy as it is able to accept data from the Internet of Things (IoT) devices and social networking sites/apps. Such voice, video, and data can then be routed to any group of users/devices through SDN (Software-Defined Networking). The Integrated Communication Platform can also be integrated with Telepresence and Video Conferencing technologies, supporting video conferencing between commanders, specialists, and frontline officers.

Another crucial component of Huawei's Safe City solutions is the Intelligent Video Surveillance, comprising Video Content Management, and Video Cloud. This component can process/analyze videos from many sources including those from social networking sites/apps. Scene search allows one to search, for objects such as a white van. Video synopsis helps to 'summarize' many hours of video into crucial clips for analysis by human investigators, which enables cases to be solved quickly. The Video Content Management feature also comes with more than 20 intelligent analytics including entity recognition, behavior, crowd counting, and virtual tripwires. The tiered Video Cloud provides cost-efficient archival of video footages at both remote sites and centralized locations. Huawei offers high definition IP Cameras that come with their own power supply too.

Existing Safe City implementations can be enhanced with various technologies such as Sensor-based Early Warning, Social Monitoring, Public Warning, and Smart Deployment. Huawei's IoT-enabled sensors, including buoys, can detect Tsunamis, CBRN (chemical, biological, radiological, and nuclear), and radar/electro-optics for border surveillance.

Public Safety

Public Safety is more than just ensuring safer cities. It is about preventing and solving crimes, reducing loss of life and property. Public Safety is also about minimizing disruption to life, and thus, it goes beyond detection and response. It includes prevention and efforts to regain a state of normalcy. It encompasses digital security, health security, infrastructure safety, and personal safety. Indeed, on personal safety, when the then British Home Secretary Sir Robert Peel established the London Metropolitan Police in 1829, he said "*The police are the public and that the public are the police.*" Unfortunately, this principle has not

been adopted by many police departments around the world for the last 180 years. In light of the disruptions brought about by the Digital Economy, this principle is now even more critical than ever. As such, we need to evolve from Safe Cities to Collaborative Public Safety.

It Takes a Network to Fight a Network

To achieve Collaborative Public Safety, we need to consider the four pillars behind the Network of good guys:

- **Inter-Agency Collaboration.** Violent extremism, crime, and even pandemics strike across boundaries and sovereign borders. All public safety agencies in a country, and across countries, have to collaborate to fight such threats. Collaboration includes sharing of information and best practices, interoperability of communication methods, and coordinated joint actions.
- **Communities Collaboration.** Partnership has always been around. The challenge is in make the partnership better or wider to meet new demands.
- **Partners' Ecosystem.** Cyber-facilitated threats in this age of Digital Economy are very much fueled by technologies. Likewise, an ecosystem of technologies is needed to enable the collaboration and partnership mentioned above.
- **Leading New ICT.** Technological solutions need to run on a secure and robust platform, supporting data, voice, video, and even IoT. With its globally proven information, communication, and networking technologies, Huawei's Leading New ICT is the fourth pillar behind this network of good guys.

Prevention is better than cure. One cannot prevent if one cannot even identify the threats. Predictive policing, or PredPol, involves analysis of data to predict the next crime, with the objective

of preventing it. With potential threats identified, governments have to enact regulations, require licensing, and carry out enforcements. Other forms of licensing and enforcement include fire safety inspection, building code, alcohol control, traffic enforcement, etc. Even Border Protection is a form of licensing and enforcement to prevent threats.

Despite our best efforts, some threats simply cannot be prevented. This is why simulations and forecasts are needed to reduce the loss of life and property. In line with the full definition of Public Safety, governments are expected to minimize the disruption to life. This is when we enter the Recovery phase.

During this phase, investigation and evidence collection are crucial for the following purposes:

- To locate victims and identify remains if there are fatalities
- To identify the responsible party and ensure that justice is served
- To learn from the threat, and to prevent recurrence

It is unfortunate that even within the investigation function, there are different specialists in a single law enforcement agency. This has often resulted in different stove-piped systems, creating inconvenience to the victims, witnesses, and even law enforcement officers. Similarly, a victim identification system is needed to identify those who are injured and their whereabouts, as well as those who have died. Families and friends of victims may pose a secondary public safety problem if they do not receive timely information about their loved ones.

To support the investigation process, a criminal intelligence system is needed to establish links between people, objects, locations, and

events, and to narrow down the suspects. With the investigation completed, an inquiry or court hearing is needed to close the loop. Rehabilitation, including punishment and imprisonment, aims to prevent the occurrence of such threats. The lessons learnt provide inputs back to the Prevention phase.

Collaborative Public Safety requires processes and technologies for Social Engagement, Crowd Sourcing and Public Communication. An interesting example is the Singapore Civil Defence Force's (SCDF) myResponder. People trained in Cardio Pulmonary Resuscitation (CPR) can register as volunteers and use the myResponder mobile app. When there is an incident involving a serious medical condition such as a heart attack for example, the SCDF control room will dispatch an ambulance, and at the same time send a message to those myResponder volunteers in the vicinity. The app will also inform the volunteers of the nearest Automated External Defibrillator (AED). Several lives have already been saved through this 'crowd-dispatch' approach.

Conclusion

In short, the good guys have to embrace the Digital Economy and form a network to fight against the network of bad guys, who are already leveraging the technologies behind Digital Economy: Social, Mobile, Cloud, and Big Data. This is the spirit behind Collaborative Public Safety, involving inter-agency collaboration and public-private partnership.

**Arthur Holland Michel**

Co-Director

Center for the Study of the Drone

Bard College

Arthur Holland Michel is an author, researcher, and the co-director of the Center for the Study of the Drone at Bard College, an interdisciplinary research and education institute that examines the challenges and opportunities associated with the proliferation of unmanned systems technology in military and civilian spheres. Mr Holland Michel is particularly interested in how stakeholders can leverage innovative research and inquiry-driven resources to get ahead of the adoption curve of emerging technologies and effectively anticipate the potential social, economic, legal, and ethical implications of these systems. He has written extensively about drones, robots, and defense for a variety of publications, including *Wired Magazine*, *The Oxford Research Encyclopaedia of Crime, Media, and Popular Culture*, *Vice*, *Al Jazeera America*, *Fast Company*, *Bookforum*, *U.S. News*, *the Verge*, and *the New York Daily News*, among other publications, and is the co-author of a number of research reports, including “The Drone Primer: A Compendium of the Key Issues,” “Drone Sightings and Close Encounters: An Analysis,” “Local and State Drone Laws,” and “The Drone Revolution Revisited: An Assessment of Military Unmanned Systems in 2016”. He is the author of a forthcoming book about airborne surveillance technology, to be published by Houghton Mifflin Harcourt in 2018.

DRONES, COUNTER-DRONES, AND AI IN POLICING: A SURVEY OF OPPORTUNITIES AND CHALLENGES

Authored by
Arthur Holland Michel

Executive Summary

In today's fluid security environment, certain emerging technologies that had their origins outside the law enforcement sphere are drawing growing interest from agencies and organizations seeking to achieve their mission more effectively. For example, police departments across the globe are turning to social media platforms as a tool for both engaging their constituencies as well as trawling for suspicious or criminal activity, while cybersecurity tools developed for the commercial sphere are increasingly finding a market among law enforcement agencies looking to fight crimes that occur in the virtual world.

Three technologies are particularly emblematic of this trend: (a) unmanned aerial vehicles, better known as drones; (b) counter-drone technology; and (c) the emerging sphere of autonomous and artificially intelligent (AI) systems. Unmanned and autonomous systems present myriad opportunities to address both law enforcement challenges that are as old as law enforcement itself, while counter-drone technology addresses an emerging threat that has largely caught the security community off-guard: rogue drone use. All three technologies will play an important role in policing smart cities of the future.

Much has been written about the potential benefits of all three of these technologies when used in a law enforcement context. And indeed, law enforcement organizations looking to remain on the leading edge of the technological curve would be remiss not to consider these tools. However, less ink has been spilled on the potential challenges involved in their adoption and effective use. To that end, this paper will enumerate both the opportunities and challenges associated

with the adoption use, and integration of drones, counter-drone systems, and AI.

Law enforcement agencies looking to adopt these types of systems can use this paper as a resource to weigh these opportunities and challenges against each other in order to support an informed decision as to whether such systems make economic, tactical, or legal sense within their own unique security environment.

Law enforcement agencies looking to potentially adopt other emerging technologies not covered in this paper, such as social media monitoring tools, bodycams, and other sensor types, might also benefit from considering the pros-cons framework presented herein as a guide for evaluating those technologies.

Drones

Benefits:

- *Drones can provide improved situational awareness;*
- *Cheaper than traditional airborne imagery collection tools such as helicopters and fixed-wing aircraft;*
- *Drones may be well-suited to search-and-rescue operations;*
- *Drones could allow officers to collect intelligence at a safe standoff distance during potentially hazardous situations;*
- *Can be used to generate detailed 3-D models of crime and accident scenes.*

Challenges:

- *Drones have far less capabilities compared to manned aircraft;*
- *As an emerging technology, drones may not be well-suited to every application that they are being used in, and there is a dearth of data about drone performance in law enforcement operations;*
- *Drone use may prompt civil liberties*

concerns, and could face regulatory and public pushback if used in certain applications such as surveillance.

Counter-Drone Systems

Benefits:

- *The malicious or improper use of drones presents a potentially serious public safety hazard, and counter-drone systems could effectively mitigate the threat;*
- *Counter-drone systems are designed specifically to identify and interdict drones, so they likely have a higher efficacy rate compared to other methods (for example, using visual observers).*

Challenges:

- *There is no single silver-bullet solution for counter-drone systems technology—different detection and interdiction systems have strengths and weaknesses;*
- *Kinetic interdiction systems may be impractical or unsafe for use at public events or in urban settings;*
- *Certain non-kinetic interdiction systems may be impractical in urban settings, as they may interfere with wireless communications;*
- *Counter-drone detection systems are ineffective at distinguishing between legitimate and threatening drone use.*

Artificial Intelligence (AI)

Benefits:

- *AI systems could improve efficiency and cut down on human labour needs by automating tasks such as hotspot analysis and imagery analysis;*
- *AI systems can enable predictive policing tactics that potentially cut crime rates;*
- *Artificially intelligent unmanned systems could replace human officers in dull or dangerous roles.*

Challenges:

- *AI systems can behave in unpredictable ways, and their use can yield unforeseen results;*

- *AI systems are complex, and errors that lead to harm may be difficult to trace;*
- *AI systems may amplify human bias in the law enforcement realm;*
- *AI systems remain unregulated, and their misuse may be met with severe regulatory pushback that limits all use of these systems.*



Dr William H. Saito
Special Advisor to the Cabinet
Government of Japan

William H. Saito named by Nikkei as one of the “100 Most Influential People for Japan”, began software programming in elementary school and started his own company while still in high school. By the time he was named Entrepreneur of the Year in 1998 (by Ernst & Young, NASDAQ and USA Today), he was recognized as one of the world’s leading authorities on cybersecurity.

After selling his business to Microsoft, he moved to Tokyo in 2005 and founded InTecur, a venture capital firm. In 2011, he served as the Chief Technology Officer of the National Diet’s (Parliament) Fukushima Nuclear Accident Independent Investigation Commission. In 2012, Saito was appointed to a council on national strategy and policy that reported directly to the Prime Minister of Japan.

He is a Foundation Board Member, Young Global Leader and Global Agenda Council member for the World Economic Forum (WEF).

Saito also advises several national governments around the globe and currently serves on the Global Commission on the Stability of Cyberspace.

THE IMPACT OF IOT ON CYBERSECURITY AND THE FUTURE OF TRUST IN THE DIGITAL AGE

*Authored by
Dr William H. Saito*

All too often, cybersecurity is something we remember to do when it's too late. We're living in an age of constant online threats but widespread complacency. Part of the problem is that technology is evolving too quickly for most people to keep abreast. Another is the sheer volume of attacks makes it difficult to see the big picture. A third is that many businesses and governments – nevermind individuals – still see security as a cost center, rather than as a business enabler.

The WannaCry ransomware attack that paralyzed hundreds of thousands of computers worldwide in May, already seems like ancient history. But like many recent attacks, it is a teachable moment: we can no longer afford to be complacent when it comes to cybersecurity, and must architect our businesses, our systems and ourselves to prevent them.

WannaCry is a form of malware that exploits a Windows vulnerability to encrypt victims' files and hold them hostage, promising to release them when a ransom payment is made. This was one of the largest, most damaging attacks we have seen in recent years, and it was also a distraction from all the other attacks happening that did not get as many headlines. So, let's learn from this. The world will continue to hear about the new "largest" and "most damaging" cyberattack as our reliance on the Internet of Things increases, and our attention must shift to security by design, not the attack du jour.

What WannaCry means for IoT

WannaCry's effects were uneven, and many weeks later, it is hard to say how impactful this ransomware really was.

In many countries, the damage from WannaCry was quite minimal due to both its design and some lucky breaks by researchers. In Japan,

for instance, initial reports said only a handful of computers were affected. What is far less known, however, is that the same vulnerability in use by WannaCry was being exploited by other actors weeks earlier in several covert operations that hijacked computers for everything from stealing information (such as credentials and credit card info) to using their processing capabilities to create cybercurrency. What was remarkable about this is that several different actors had managed to unleash a large but hidden attack that went undetected for several weeks and it was only exposed when others used the vulnerability to launch a very public ransomware heist.

In most cyber attacks, developing the delivery system to get the malware onto a target is the hard part. In the case of WannaCry, the payload portion (ransomware) was not unique and in fact was poorly written. The delivery system, however, was of a professional grade computer code that allowed even beginner programmers to "bolt on" their payload of choice. WannaCry is another example of how a sophisticated cyber weapon became available to anyone and was quickly exploited for criminal gain. As noted many times, that accessibility has been a seismic shift in the cyberattack landscape over the past decade – tools that were once the province of only sophisticated attackers are now readily available for use by novices.

This is not a time for complacency. Many attacks in the future would not be so obvious, and many will be even more nefarious than WannaCry was. In the future, IoT devices will only add to the complexity of this system as many different vulnerabilities, as there are manufacturers, will be found in them. Attackers only need to find a delivery system based on a vulnerability to establish a foothold within a network to carry out their main attack with a separate payload.

Here is an example. If I can find a weakness, such as a default password, in a particular IoT device in your network that is doing something benign, such as turning on a light, I can take over that device and use it as a beachhead over a long period of time to deploy other external payloads (both newer or specific to the target) and keep on attacking from within the firewall. All this happens from an area that is outside the reach of your machine's antivirus scanner. In one reported instance, a university's computer network was attacked when over 5,000 of its own IoT devices ranging from vending machines to light sensors flooded its servers with requests for information, slowing the system and restricting internet services. If such incidents continue unabated, IoT will soon be renamed "Internet of Threats" or "Insecurity of Things," and as a society, we cannot afford that. Outmoded technology such as antivirus – which cannot possibly keep up with the range and sophistication of threats being delivered to endpoints such as PCs and mobile devices – is only part of the problem.

A positive effect of the WannaCry attack is that it immediately raised awareness about the importance of cybersecurity among victims and non-victims alike around the world. People running unsupported Windows XP operating systems realized how vulnerable they are and then benefitted from an emergency patch from Microsoft. Even Mac users were reminded to update their OS and antivirus programs and consider more advanced endpoint protection. This happens every time we have an Iloveyou, or Stuxnet, or another form of headline-grabbing malware that dominates the news cycle. Because of these incidents, consumers tend to have their computers on "auto update" and thus, were already protected from the known vulnerability that WannaCry exploited. Unfortunately, the difficulty and disruption caused by patching systems in business or critical support roles means that updates are often not automatic; that is why many more

users in the business and services industries were affected. In the new world of IoT, this lesson is food for thought: that resilient IoT systems need responsible manufacturers who maintain security patches for their IoT devices and update them in a transparent fashion without disruptions to the end user's experience.

Moore's Law and threat multipliers

Moore's Law is an important consideration for where we've arrived with securing IoT. Formulated by Intel founder Gordon Moore in 1965, it holds that the number of transistors on microchips doubles every two years. The law has actually "existed" for the last 100 years since the advent of the mechanical calculating machine and has basically held true since then. The law has miniaturized transistors, sped up communications and increased storage space and developed an array of useful sensors. Nowadays, with the advent of IoT devices, we are seeing sensors and wireless communications modules being deployed on everything from refrigerators to oil pipelines, bringing millions of machines, including much critical infrastructure, online. IoT allows combinations in Moore's Law that were not possible in the past due to size and cost. But more importantly, because sensors are so cheap now, it is the first time in ICT history where we actively use data that has not been manually entered, created, calculated or manipulated by humans. Automatic devices are now doing the job, and the result is an extended web of sensors feeding an increasingly vast lake of data.

Another effect of Moore's Law has been an ever-decreasing cost of computing power. The doubling of power may not have been noticeable in the early days of computing, but now it produces tremendous effects. The phones in our pockets today have sophisticated sensors that would have cost hundreds of thousands of dollars only 10 years ago instead

of only hundreds today. Just a decade ago, the five most valuable companies in the world were in oil related industries. As of 2017, all five companies are now information technology companies. Data is the new oil. While oil changed the world in many miraculous ways, it has also created headaches that still exist today. The same is true of data. We are generating enormous volumes of data through technologies such as mobile devices and IoT. Who owns this data, and how is it being used? Privacy has emerged as a major issue in protecting life in the digital age as user data has exploded and become commoditized.

Greater computing power, however, allows cybercriminals and bad actors to launch increasingly frequent and sophisticated attacks. Unlike threats of the past, bad actors that do not even have the capability to develop their own tools can use existing malware and exploits that are often free or inexpensive to obtain online. Sophisticated actors are also developing and selectively using unique tools, such as custom malware, that could cause even greater harm. This all adds up to tremendous leverage for the attackers.

Sadly, many companies are still relying on decades-old core security technology and favoring remediation – assuming an attack will take place and cannot be stopped – over prevention. Worse, from a technology product standpoint, most companies and governments have over a period of decades acquired and stitched together point products designed to address only specific challenges in security, which severely limits overall visibility and weakens their overall security posture.

When taking security measures, many companies focus on safety and costs, while paying less attention to convenience, but if companies could realize the concept of “security by design” and give sufficient consideration to convenience, executives

would surely be able to utilize security as an effective tool to enhance the corporate value of their organizations, rather than seeing it as a cost center or a liability.

Furthermore, developers of IoT devices need to create a security monitoring and update paradigm for their products, including products long past their physical warranty dates, to keep them patched and up-to-date automatically and transparently. While the last generation of computing products and service manufacturers did not realize and reflect the extent to which their technologies were going to be networked and used, in today’s world safety and security must be built in with all known and unknown use cases in mind.

And there is one more thing worth mentioning, which is that organizations cannot hire their way out this challenge. Putting aside the worldwide conundrum that demand for cybersecurity skills way outstrips supply, even if organizations could hire everyone they wanted to, more headcount to manage legacy architecture would not bridge the gaps between point products or siloed technologies. Everyone in our industry talks about “platform,” and that is often a marketing term. But a true next-generation security platform is one that embraces that “security by design”: natively integrating security capabilities, sharing important context, offering complete visibility, and automatically reprogramming itself to account for new threats.

The important takeaway from all this, including the WannaCry attacks, is that we have to change our thinking about IT to adjust to this new reality. Cybersecurity is just as important as health and personal safety – keeping your computer system updated and patched against the latest threats has become critical as IT plays an increasingly central role in our data-driven lives. We can modify our online behavior

to treat data as we would treat food, never ingesting morsels that might be suspect and possibly toxic. We can observe any number of cautionary practices from data backups to multifactor authentication to minimize risk, but it is equally important to cultivate a mindset of resilience through which we can recover and keep operating when we do become victims of an attack.

Attacks can come anytime and attackers never sleep, but we do not have to make their jobs any easier.

We really can make it so cost prohibitive for them to attack such that the economics just do not add up.

We really can shift the discussion at industry conferences to action by willing governments, working with the private sector – long talked – about, but finally happening in 2017.

We really can architect for prevention, and use technology that can prevent both known and unknown attacks while using the information from discovered attacks to become even “smarter.”

We can educate our employees, friends, families and governments to be more cyber-aware, and understand just how much has changed in such a short time. We can preserve trust in our digital age through the right combination of people, process and technology.

Everyone is talking about cybersecurity when something like a WannaCry happens; we cannot waste this opportunity to meaningfully advance.

It is important to note that these trends will also weigh heavily on how law enforcement operates today and in the future. Preventing cyberthreats and stopping cybercriminals

requires both offense and defense, with national and global agencies such as the U.S. Federal Bureau of Investigation (FBI), Britain’s Government Communications Headquarters (GCHQ) and INTERPOL working closely with partners and the private sector, including security technology vendors.

Shared threat intelligence is also critically important. Several major partnerships are in place already, including the Cyber Threat Alliance, which includes industry vendors that have chosen to work together in good faith to share threat information, for the purpose of improving defenses against advanced cyber adversaries. There is also the work being done by the Global Commission on the Stability of Cyberspace (GCSC) and the International Institute for Strategic Studies Asian Security Summit, among many others.

What is clear is that cybersecurity is becoming increasingly prominent at gatherings of senior officials and in forums where in the past more traditional discussions of defense and law enforcement have dominated the agenda. All of this bodes well for law enforcement agencies taking a more proactive stance with cybersecurity as often as they are reacting to cybercrime.



Kris Ranganath
Senior Director
Advanced Recognition Systems
NEC Corporation of America (NEC)

Kris oversees product development, research, and technology integration for public safety solutions at NEC Corporation of America (NEC), a leading provider of IT solutions, and advanced artificial intelligence enabled recognition systems for enterprise and public sector markets. Kris has over twenty-five years of experience in developing solutions for city, state and nations with emphasis in identification, immigration, intelligence and investigation technologies.

Prior to this, he held the position as CTO of NEC Government and Public Global Solution Division, this division provides biometrics, and analytics enabled public safety solutions around the world using multiple solution centers in different geographic regions.

Kris actively participates in standards specifications and has presented in several global security conferences. He strives at integrating latest innovative technologies to address current and future public safety demands.

AS SMART CITIES TRANSFORM, SAFETY AND SECURITY COME FIRST

*Authored by
Kris Ranganath*

Standfirst: Getting to the heart of today's security challenges means adapting mindsets, strategies and operational procedures.

As the Fourth Industrial Revolution gets underway, there is much talk about digital transformation in both the private and public sectors. City planners and government agencies are looking to e-services that can boost the quality of living for citizens.

At the same time, ever changing security scenarios demand that they use an ambient computing environment to monitor, investigate, analyze, predict, and forecast threats from ubiquitous data, media and sensors.

Today, advances in recognition technologies, video analytics, the Internet of Things (IoT) and artificial intelligence present unique opportunities for public agencies to undergo digital transformation. This enables them to address changing security threats, while creating a secure and healthy environment for citizens to thrive.

One issue is that a lot of today's efforts are conducted individually. One agency or branch of government may roll out a solution to solve its problems but it may not be connected to other related services. The result is a lack of coordination and a failure to optimize one's investments.

For example, a police department may start setting up a video surveillance solution to help it monitor areas with a high incidence of crime. Separately, a fire department may deploy a fire alert solution to warn it of an emergency.

And what about the energy department, which may have building energy management systems (BEMS) in place. Or a traffic

department that installs a congestion prediction system?

These operations running parallel and in silos mean that each agency only aims for specific, individual outcomes based on their own missions and budgets. This makes it hard for a city leader to realize his high-level objective of improving his citizens' lives.

The challenge is more urgent now because of the increasing pressure that a growing urban population brings to bear. Globally, the number of people living in cities is set to grow from 3.5 billion to 6.3 billion, a 1.8-fold increase.

Separately, the movement of people will grow two-fold, the movement of things, such as consumer goods, would grow 2.4-fold and the demand for food will increase 1.7-fold.

What this means is increased stress on physical and digital infrastructure. Trains will have to move faster and carry more people. Networks will have to deliver more data in a world of smart sensors.

As cities become more connected, the biggest challenge maybe not be getting the right IoT or artificial intelligence (AI) technologies but making the most of a fixed budget and untangling complicated stakeholder structures.

Breaking down silos

In some countries, the approach has been to break down silos between agencies and roll out more efficient safer city innovations. Instead of having each party work on its own solutions, a more holistic strategy leads the way.

In Wellington, New Zealand, for example, the city council decided early on that it wanted inter-agency collaboration for its rollout of an

IoT platform. Data would be shared among agencies to resolve key issues such as anti-social behavior, congestion and pollution.

The sensors today collect and analyze information such as the number of cars in an area and the quality of the air. Cameras are also able to pick up unsocial behavior.

A similar collaborative effort was rolled out in Christchurch in the same country. Here, the city wanted to develop a smart city block where car parking, street lighting and pedestrian mobility could be monitored, along with air quality.

This gives the city leaders a better understanding of pollution and congestion, enabling them to make decisions based on actual ground evidence.

The two cities are part of a smart nation project led by Land Information New Zealand (LINZ). Besides data, it encourages cities to share good data practices that can improve communities.

The same type of collaboration is also carried out in other cities around the world, where it is vital to have an integrated approach to make use of the information streaming in from cameras, sensors and other connected devices in the field.

In Tigre, Argentina, the key objective of a new central command center is to keep the city safe, healthy and friendly to tourists, thus creating jobs in the sector.

In a highly connected hub, information is pulled from systems across the city. Established in 2014, it brings together the police, fire department, the judiciary and citizens, who can also provide on-the-ground feedback of any suspected criminal activities.

License plates are recognized from camera images fed to the center. Faces are also recognized by state-of-the-art technology that can detect and track people of interest, including suspects of a crime.

And even before a crime is committed, individuals in a high-crime area can be monitored for behavioral cues that may signal, say, an impending car theft.

By tracking and deterring crimes more efficiently, the law enforcement agencies in Tigre have helped reduced car theft by 80 per cent. At the same time, the number of visitors has grown 20 per cent a year to a record-high in 2015.

Perhaps more importantly, citizens trust that the city government is doing a good job in making city life safer.

Yet another case study is Singapore. Often cited as a living laboratory for the latest innovations, the country has been exploring safe city technologies for several years.

In 2014, it set up a test bed to pilot cutting-edge video and acoustic analysis technologies, as well as combined cyber information surveillance for predictive policing.

Key to this setup, once again, was inter-agency collaboration. The combination of both physical and online sensors means that the information streaming in has to be made sense of.

For example, cameras analyzing 230,000 faces a day were able to detect a person loitering repeatedly at a monitored location. This was done by understanding the various locations he had been to and tracking him across multiple cameras.

Other behavioral analysis can be carried out, for example, to detect congestion on a subway

train platform, screaming and shouting or other unusual crowd behavior, such as people suddenly falling on the floor, perhaps as a result of a gas attack.

At the same time, cyber surveillance would help detect possible signs of an impending attack over social media, for example, pre-warning the authorities of a possible emergency to prepare for.

More than the technology, what the Singapore test bed demonstrated was the ability for multiple agencies to work together. No fewer than seven agencies were involved in the trial, including the police, environmental, transport and homeland security agencies.

Technology not a silver bullet

Though technology is the catalyst that creates the breakthrough, it is not a silver bullet that solves all problems.

Rather, it is a way to encourage more agencies to get onboard and collaborate, after they have seen a visible outcome in one agency.

Working with many government partners over the years, from implementing biometric-based immigration control systems to delivering surveillance and analysis technologies, NEC has gained much experience with the challenges faced by cities around the globe.

If various agencies were to work within their own objectives, then a lack of coordination and a clearly mapped-out strategy could potentially affect the success of a smart city rollout. That is not even mentioning the overlapping areas that result in inefficiency and a waste of resources.

To realize real-world benefits from safer city solutions, it is crucial to change the mindset of siloed budgets and solutions aimed at solving individual issues. A more holistic approach has to be drawn up.

What some cities, such as Singapore, Tigré, Christchurch and Wellington, have demonstrated is the importance of collaboration across agencies.

This is enabled by AI and IoT solutions that are based on a data-centric platform. In future, providing access to this platform to the relevant agencies will be a key step in helping break down the walls. With that in place, we can kickstart the much-desired digital transformation in a government.

Find out more about NEC's business intelligence at Booth #963 Contact y-mochizuki@az.jp.nec.com (LinkedIn: Yasunori Mochizuki)

**Yuval Ben-Moshe**

VP of Forensics Business Development
Cellebrite

Yuval Ben-Moshe is the VP of Forensics Business Development at Cellebrite, the world's leading provider of digital forensic solutions. Mr Ben-Moshe is a subject matter expert for the company and a central knowledge hub, fostering the company's tight and intimate relationship with the forensics community of law enforcement agencies worldwide. Mr Ben-Moshe has an accumulated experience of over 25 years, heading many technological and business initiatives, with leading and innovative companies, mastering fields of security, cellular communication and cutting-edge software systems. Mr Ben-Moshe is Cellebrite's primary speaker and representative and as such, holds an irreplaceable view of the global markets and professional trends.

RETHINKING THE INVESTIGATIVE PROCESS

Because every byte matters

*Authored by
Yuval Ben-Moshe*

Summary

A typical person's digital profile contains an extensive amount of data about their lives, thoughts, plans and connections. For investigators, digital data is a gold mine of evidence. Yet, with the extensive growth in the volume and complexity of digital data, getting to the data can be challenging and law enforcement agencies must rethink the investigative process and embed an end-to-end digital investigation workflow from the get go.

Digital devices, mainly smartphones and tablets, have become an integral part of peoples' daily lives, and it is no surprise to see that they have surpassed computers. They are used for everything, including: communicating (via a regular phone call, an SMS message or Whatsapp); posting information to social media channels such as Facebook, Twitter and LinkedIn; exchanging photographs; watching and recording video and audio; browsing the internet; writing notes, navigating, making payments and much more.

But in the wrong hands, criminals will take advantage of the technology and the people connected to it to facilitate a criminal activity. Sexual predators will often use digital devices to make initial contact with their victims, groom them, and exchange photographs or videos. Digital devices are also instrumental in homicide investigations, used by gangs to coordinate drug deals, to smuggle contraband across borders. Encrypted chat applications are frequently used by terrorists and major criminal organizations to communicate and share information, coordinate activities, and spread propaganda via social media channels. Yet, without knowing, they are creating a vivid cyber track for digital investigators to follow. As a result, **digital data has become a key component in criminal investigations.**

With the investigation clock ticking, and the extensive growth in volume and complexity of digital data in mobile devices, on the cloud and other digital platforms, law enforcement need quick and easy methods to dig deep into the details to find answers, and provide context around specific events related to both victims and suspects, to plan their next steps. They need information they can act on immediately. However, with mobile devices increasing in functionality, as well as the various file systems, data formats and sources out there, accessing the data can be challenging.

The 48-hour mark

It is a common understanding, that the first few hours of an investigation are the most crucial for obtaining solid leads before the chance of solving a case drops by fifty percent.

For this reason, quick access to actionable evidence through digital investigative techniques, is critical. However, with technology continuing to evolve at a blinding pace, digital investigation capabilities have reached a tipping point, forcing law enforcement agencies to rethink the investigative process. Agencies can no longer withstand the overwhelming volume of data with the few resources they have. Proven and scalable investigation solutions are needed to quickly obtain, analyze and share information in order to reduce time to evidence and solve cases fast.

“The time has come to rethink the investigative process and the tools required to support it.”

A fundamental understanding that drives this change is that digital evidence must be embedded into the End-to-End Digital Investigation process (EEDI). EEDI presents a new way of thinking, breaking down the silos *modus-operandi*, in which digital investigations are carried out - by technical specialists in closed labs. The EEDI leverages on modern tools and solutions, empowering investigators to conduct certain elements of the digital investigation process.

With it being such a fundamental change, the EEDI requires leadership and vision, detailed plans, and management control. To assist with such leadership, we are offering the key success factors, that should be at the crux of the change for it to be effective:

1. Regular Key Performance Indicators (KPI) Reporting and Control

A force-wide, multi-stakeholder End to End Digital Investigation (EEDI) involving thousands of users, would require strict efficiency monitoring and management, with strict user administration controls. Building the right metrics from day one, organized in a form of Key Performance Indicators (KPI) and monitoring tools are essential foundations for such management to be efficient and effective. These tools would provide timely information amongst users and the deployed tools, while administration controls would always have a clear and concise way to monitor performance and efficiency.

2. Multi-Tiered Structure

Exhibits backlogs, waiting to be processed by central labs put cases in jeopardy. Law enforcement agencies must implement a more distributed workflow outside the central lab to reduce the backlog and increase the 'case closed' rate.

Empowering officers and investigators in the field to collect, analyze, share and act on critical digital data findings is now possible with modern investigative tools and solutions that are simple to operate without jeopardizing any of the strict forensic rules.

Distributing the workload across the force and the investigative team, reduces backlog, speed investigations, and quickly places the digital intelligence in the hands of those that need it the most.

3. Ongoing Digital Forensic Capabilities and Technological Updates

Keeping up with the volume, complexity, and speed of change in digital data is challenging. With OS's and devices entering the market at a blinding pace, and new social applications launched daily, it is critical to have a reliable and feasible plan in place. This is to assure that all digital investigation platforms and solutions can support the technological developments of today and are ready to face the changes of tomorrow. The key is to approach the EEDI as an ongoing campaign that aims to always be one step ahead. How? By partnering with trusted vendors that are committed to always keeping them up-to-date with the latest capabilities that affect any changes and developments related to digital technology.

4. Ongoing Development of Skills and Knowledge

The same way the platforms and solutions need to be updated with the latest extraction, decoding, analysis and reporting technology, so do the people handling them. A plan for training, certification refreshers and recertification is critical to always keep the professionals at the forefront of technology.

By teaming up with the best and most accomplished professionals in the industry, investigators, examiners, and other law enforcement personnel retrain and refresh on a regular basis to fulfill their potential and achieve their goals.

5. Information Sharing and Collaboration

When working on a case, a collaboration between teams, individuals, and cases are crucial to finding the specific piece of evidence that could speed an investigation. With the right tools in place, consolidated insights, from single or multiple sources as well as cross case collaboration, when needed and allowed, can help investigators see both the bigger picture and all the critical connections. To do this, users need reliable data management tools implementing advanced investigative engines, in addition to cutting-edge algorithms designed specifically for text and media relevant to specific investigations.

6. Unlocking the Intelligence from Within

The majority of investigations today start with the acquisition of data from digital devices. But when a device is locked, damaged, or contains unknown application data formats and encryption technologies, it could delay the investigation process before it has even begun. Getting past this barrier becomes the critical first step.

Even with the most sophisticated digital forensic tools, additional expertise and skills may be required to access the data to surface critical insights that may have otherwise been missed.

In summary, keeping pace with digital evidence is vital to the mission of keeping communities safe. Agencies that implement the new End-to-End Digital Investigation

processes and optimize workflows, gain a critical advantage in the fight against crime.

As a trusted partner to law enforcement agencies around the world, Cellebrite is committed to helping agencies tackle these considerable challenges with the technology, training, and support necessary to harness digital evidence both today and for many years to come.

**Valdecy Urquiza**

Brazilian Federal Police Commissioner
Head of INTERPOL Brazil

Valdecy Urquiza is Head of INTERPOL's National Central Bureau in Brazil. He previously worked as Federal Police Coordinator-General of Information Technology and led the Brazilian delegation in the Mercosur Group of Specialists in Information Technology and Communications between 2010 and 2014. Urquiza is also a professor at the National Police Academy. He has subject-matter expertise in the following disciplines: Public Administration (from Ibmec University), Environmental Law and Strategic Sustainability Management (from the Pontifical Catholic University of Sao Paulo - PU /SP), and Criminal Justice (from the University of Virginia, USA). He is also a graduate from the FBI National Academy in Quantico, Virginia.

THE USE OF TECHNOLOGY AND COLLABORATIVE APPROACH TO TRACK TERROR THREATS (RIO 2016 OLYMPICS)

*Authored by
Valdecy Urquiza*

The task of ensuring safety at the biggest sporting event on the planet was not easy. The numbers from Rio 2016 Olympic Games are impressive. Close to 11,400 athletes, 45,000 volunteers, 25,000 journalists, 3,200 referees and sporting assistants from 205 countries gathered in Brazil for the event. More than a million and a half tourists went to Rio de Janeiro to follow the competitions, including half a million foreign tourists. In addition, about 40 foreign authorities, including heads of state and ministers, attended the official opening ceremony of the games.

According to a study published in 2016 by the non-governmental organization Citizen's Council for Public Security and Criminal Justice International, Brazil is the country with the highest number of violent cities in the world. Of the 50 cities with the highest homicide rate per 100,000 inhabitants in 2016, 21 are Brazilian.

The city of Rio de Janeiro, with its nearly seventeen million inhabitants, struggles every day with domestic issues such as lethal robberies and urban drug war violence.

The increase in transnational crime is undeniable, with the emergence of new forms and methods of delinquency, in an increasingly globalized environment marked by the breaking of barriers and the rapid circulation of people, information and money around the world.

Brazil has no history of terrorism committed by Islamic extremists. But major sport events are often a potential target for extremists, especially when one-third of the countries participating in the Games are also members of the international coalition fighting the Islamic State. The Olympics Games have faced

various threats since 1972 when terrorists killed 11 Israeli athletes during the Games in Munich.

Given this peculiar scenario, hosting the Olympic Games in Rio de Janeiro represented the biggest challenge ever faced by police agencies in Brazil. It is the largest police operation in the history of Brazil, comprising the deployment of 85,000 police officers.

To guarantee safety at the Games in Rio de Janeiro, the Brazilian Federal Police needed to adopt new strategies that would allow precise and efficient intelligence-gathering.

To this end, the Brazilian Federal Police implemented the International Police Cooperation Centre (IPCC), which was a Command and Control Center located in the heart of the city of Rio de Janeiro.

The first, and perhaps the most relevant, characteristic of the IPCC was its collaborative approach. Together with 220 Brazilian federal police officers, 250 police officers from 55 other countries worked at the IPCC. These police officers carried out intelligence analysis and the production of intelligence reports that were disseminated to the various police agencies involved in the safety of the Olympic Games.

The IPCC hosted a gigantic database composed of information from various other institutions, both public and private. This database included information from applications for accreditation to access Olympic venues and names of people who purchased tickets to attend the competitions. It also included information from open sources such as social networks, as well as information from foreign police officers who were members of the IPCC.

The Advanced Passenger Information (API) system was widely used to check international passenger lists. Whenever a flight had Brazil as destination, its passenger manifest was sent to the Brazilian Federal Police by the time the aircraft's door was closed. When the aircraft is in flight, the IPCC team conducted an analysis of all passengers on board, including crew. This check was carried out on all flights coming to Brazil, in order to identify people who could pose a threat to the country. The main objective of this check was to prevent the entry of people who might present a safety risk to the Olympics.

Cross-checks were conducted using data from INTERPOL such as the Red Notices. A Red Notice is a request to locate and provisionally arrest a person with a view to extradition. It is issued by the INTERPOL General Secretariat at the request of a member country or an international tribunal based on a valid national arrest warrant. IPCC also used the Foreign Terrorists Fighters database which stores information on several thousand people who are suspected of having joined the Islamic State. In addition, INTERPOL's Stolen and Lost Travel Documents (SLTD) database, which gathers information on over sixty-eight million missing travel documents, was also used for cross-checks at the IPCC.

Whenever a person who could pose a threat was identified on board a flight bound for Brazil, trying to get a ticket or a credential to the games, IPCC activated the Federal Police's immigration units, as well as the Federal Police's Integrated Anti-Terrorism Center. Once it was confirmed that the person was on the INTERPOL database, for example, he was prevented from entering the country or detained for the purpose of extradition.

During the Olympic Games, the officers at IPCC analyzed more than two and a half millions international passengers. This process led to

the identification of 2,700 persons of interest. Most of these people were denied entry to Brazil as their application for credentials was not approved or they were denied boarding.

In addition to checking the passenger manifests, IPCC carried out biometric examination of foreign passengers. A portable biometric identification solution called ALETHIA was developed by the Brazilian Federal Police. The solution, composed of a fingerprint scanner, an Ultrabook and a mobile phone, uses fingerprint data from INTERPOL's Red Notices and Foreign Terrorist Fighters databases. Each ALETHIA device can carry up to 100,000 fingerprints and takes less than 3 seconds to process a fingerprint, making it an efficient tool for biometric checks on the scene. ALETHIA was used to check almost five hundred thousand passengers upon arrival at the six international airports in Brazil.

To support security operations at the Olympic Games, IPCC also used two thousand closed-circuit television (CCTV) cameras that were installed in the city of Rio de Janeiro. In addition, four surveillance balloons were put into operation. The balloons, originally developed for military use, could operate continuously for up to 72 hours. Each balloon carried 13 CCTV cameras and could fly at altitudes of 200 meters above sea level. Together, the balloons supported the city-wide aerial surveillance of the city of Rio de Janeiro. All the images captured by the CCTV system were stored and analyzed. In order to effectively analyze the massive volume of data captured and enable the detection and tracking of threats, an automated video analytics system was used. The system was configured to detect changes in patterns, abandoned objects and changes in crowd flow directions. The police officers involved in the video-monitoring activity received real-time alerts every time the system detected an unusual situation. The use of the video

analytics system allowed the police officers to focus their activities on the analysis of possible threats in order to ensure prompt and effective response to any incidents occurring in areas of operational interest.

The Rio Olympic Games was one of the safest games in the history of the modern Olympics. There were no serious security incidents. This was made possible mainly due to new technological solutions that were adopted for the first time by law enforcement agencies in Brazil.

As modern-day criminals are taking advantage of the newest technologies and discovering innovative ways to act in an increasingly open and borderless society, it is vital for the Police to ensure that they could stay step of criminals. In today's world, this could only be achieved if law enforcement agencies adopt new technologies solutions such as those that leverage Big Data analysis, Long Term Evolution (LTE) networks and Internet of Things (IoT). Equipping police with digital technologies that enable fast, intelligent and accurate access to information is key to ensuring the safety of urban centers and global cities of the future.



Jorge R. Rodriguez
Commander
Los Angeles Police Department

Commander Jorge R. Rodriguez has been serving the citizens of Los Angeles for nearly three decades. Appointed to the Los Angeles Police Department in November 1987, he has successfully risen through the ranks while assigned to a variety of assignments, which included patrol, gangs, foot beats, special problems unit, detectives and narcotics. In 2001, he returned to Metropolitan Division where he was assigned to the administrative platoon, both crime suppression platoons, and as the supervisor overseeing the security details for Mayor's Hahn and Villaraigosa.

In May 2006, he was promoted to the rank of Lieutenant and returned to Rampart Area where he was assigned as a watch commander and a district lieutenant responsible for repressing crime and serving the communities of Pico-Union and McArthur Park. In October 2010, Captain Rodriguez was promoted to the rank of Captain, where he has served as a Patrol and Area Commanding Officer in 77th Street, Foothill, Topanga, and his most current assignment in Newton Area.

As a command officer, Commander Rodriguez championed a community-oriented policing style that promoted community service and collaborative relationship building. While at 77th and Foothill Areas, he developed a Hispanic Outreach collaboration initiative, in order to communicate with and educate the immigrant communities on public/police relations. He was instrumental in developing a variety of educational forums which empowered the community to act, while creating an environment that built trust between the Department and the immigrant communities. Additionally, as a champion for inner City and underprivileged youth, while assigned to Topanga and Newton Areas, he created a robust Police Activities League, consisting of a variety of programs and activities, providing the youths with opportunities they would otherwise not experience.

A PRACTICAL GUIDE TO PREDICTIVE POLICING IN LOS ANGELES

*Authored by
Commander Jorge R. Rodriguez
Mary Woodard, PredPol*

In spite of recent headline-grabbing increases in crime rates in some places, street crime remains at the lowest point seen in decades. In Los Angeles, California, for example, homicide rates in 2016 were 73% below their peak in 1992. Similarly, in the United Kingdom, property and violent crime totals in 2016 were 40% lower than their peak in 1995. While the statistics suggest that we are living in an exceptionally safe time compared with decades' past, crime still exacts a heavy toll. Consider that a single homicide is estimated to cost society at large as much as \$8.9 million and a single residential burglary \$6,462. Aggregated over all crimes, the costs are staggering. The benefits to further reducing crime beyond their current historical lows are clearly substantial.

The ideal solution is to stop crime before it happens. Calls for a focus on crime prevention are nothing new. What is new is the development of algorithmically driven crime forecasting, which makes crime prevention broadly achievable at relatively low cost, and importantly, something that police can do as part of their daily routines. Predictive policing requires two things, accurate crime forecasts and effective interventions that make crime more difficult to commit. Police already have a very good idea of where crime is most likely to occur, typically outperforming random predictions by a factor of 3 to 1. Studies in Los Angeles, California, and Kent, England, for example, show that the latest in algorithmic crime forecasting can more than double the amount of predicted crime, beating random standards by a factor of more than 6 to 1.

Knowing with greater accuracy where and when crime is likely to occur is only half of the battle. Preventing crime requires police to use those forecasts in decisions about

how to allocate their available time. Many of those decisions are actually made at the street level by police patrol officers as they encounter and deal with problems. Algorithmic crime forecasts augment rather than replace the roles played by knowledge, skills and experience of police constables in anticipating crime. Predictive policing missions that make up as little as 5% of police units' patrol time can double the amount of crime prevented. In cities as different in size as Los Angeles (~3.9 million people) and Modesto (201,000 people), California, double-digit crime reductions followed the deployment of predictive policing without subtracting from all of the other responsibilities police have. Predictions put police in the right place at the right time where they can use their judgement about the best tactics for that setting to make crime less attractive.

Predictive policing may set off alarm bells in relation to surveillance and civil liberties. Here the details do matter. There is a big difference between predicting where and when a crime is most likely to occur, and predicting who is most likely to commit a crime. There is also a big difference between using risk factors to predict crime and verify past crimes. It has long been known that *location* is a far better predictor of crime than *person*, yet the idea that we should be targeting individual offenders has persistent appeal. Knowing where crime is most likely to occur creates opportunities for police to improve local conditions, sometimes simply by their mere presence, and make crime less attractive. Knowing who is most likely to commit a crime implies interventions with individuals with the potential for direct civil liberties violations. We all know the world is now awash in data and many forms of data

— age, sex, socio-economic status, country of origin, activity patterns and personal preferences — may be risk factors for crime. Yet risk factors are themselves not criminal, and therefore the gathering of such data and their use to predict crime (especially who is likely to predict a crime) is problematic. Using the locations and times of verified past crimes to predict future crimes is not problem free, but since most reported crimes come to the attention of the police from the public we can at least say that predictive policing is being responsive to public demand.

Predictive policing shows promise in driving down crime to further record-breaking lows, but it will not prevent all crime. As much as we would wish for a zero-crime-world, this is truly beyond anyone's reach. Predictive policing makes the choice of which locations to police much more effective, but police cannot be everywhere at all times. In the absence of infinite police resources, it is inevitable that crimes will occur in the natural gaps in police patrols, algorithmically driven or otherwise.



Muhammad Faizal Bin Abdul Rahman

Research Fellow

Centre of Excellence for National
Security (CENS)

S. Rajaratnam School of International
Studies (RSIS)

Muhammad Faizal is a Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). He holds a Bachelor of Business Administration (with Merit) from the National University of Singapore. Prior to joining RSIS, Faizal served with the Singapore Ministry of Home Affairs where he was a Deputy Director and had facilitated international engagements with foreign security counterparts. He also had postings in the Singapore Police Force where he supervised and performed intelligence analysis, achieving several commendation awards including the Minister for Home Affairs National Day Award (2009) for operational and analysis efficiency; and in the National Security Research Centre (NSRC) at the National Security Coordination Secretariat (NSCS), where he led a team to research emergent trends in domestic security and monitor terrorism-related developments. Faizal also has certifications in Counter-Terrorism, Crime Prevention and Business Continuity Planning.

SMART CCTVS: THIRD EYE OF SECURE CITIES

This article first appeared in RSIS commentary

*Authored by
Muhammad Faizal Bin Abdul Rahman*

Synopsis

Many cities around the world are exploring the use of Smart CCTVs as advances in Artificial Intelligence (AI) offer operational value for homeland security. However, cybersecurity and overreliance could impede the technology's potential.

Commentary

FOLLOWING RECENT terrorist incidents, Germany's Interior Minister announced in August 2016 that CCTV cameras at airports and train stations will be enhanced with facial recognition technology. Likewise, the New York Police Department has developed the Domain Awareness System that uses similar technology to track and monitor potential suspects.

Globalisation increases the exposure of cities to myriad transnational threats even as growing urbanisation is putting the strain on law enforcement by increasing the densities of population, property and critical infrastructure to be safeguarded in each precinct. These inherent challenges in protecting cities - population and economic centres that make attractive soft targets - necessitate the early warning and identification of threats. Smart CCTVs support this function as the third eye of cities by complementing the vigilance of police officers and the community.

Securing Smart Cities

CCTV surveillance of public spaces has been a routine security feature of urban environments since the 1990s but grew in ubiquity post 9/11. Premised on the concept of "defensible space", it is a physical expression of the community's ability to defend itself against perpetrators and over time grew in importance as the "fifth utility" alongside critical infrastructures: water, gas,

electricity and telecommunications. Past incidents have demonstrated its utility in post-event investigations and disruption of further threats.

Advances in AI are improving the accuracy of video analytics - facial, behavioural and object recognition - therefore increasing the potential of Smart CCTVs to fully/semi-automate the processing and analysis of voluminous data collected from a vast network of cameras and in the long term decision-making. Smart CCTVs are capable of round the clock city-wide intelligent surveillance and not subjected to human limitations.

Countries are increasingly embracing Smart CCTVs as a quintessential feature of smart cities to meet evolving security needs given the changes to the character of cities due to growing urbanisation. For example, the Police Camera (Polcam) project which deploys CCTV cameras extensively in residential towns is a key feature of Singapore's Smart Nation initiatives and enhanced counter-terrorism strategy.

Private security firms have also begun adopting the technology to reengineer business processes by optimising security patrols with remote surveillance of their clients' properties.

Securing Smart CCTVs

While smart technologies are expected to bring benefits to modern cities, it also introduces vulnerabilities. Interconnectivity by nature enlarges the potential attack surface of cities and reveals novel attack vectors for threat actors to exploit. The hacking of the police-operated CCTV system during the 2015 Southeast Asian Games in Singapore demonstrated the plausibility and criminal intent to target law enforcement agencies.

In February 2016, Hezbollah's Al-Manar television station's claims that the militant group had purportedly hacked into CCTV cameras in Israel demonstrated a hostile intent to undermine CCTV systems as part of larger information warfare to undermine the Israelis' sense of security.

Therefore, the spectrum of cyberattacks on a city's Smart CCTVs could range from sheer criminality to compromising national security, given that cyberspace is the fifth dimension of warfare and cities are the lifeblood of nations.

Cybersecurity risk management should begin with assessments of the four aspects of plausible cyberattacks - as highlighted in a study on Smart Insiders by Oxford University, UK - namely: assets targeted, threat actors, outcomes of the attack, and attack vectors. Security policies and mechanisms should aim to protect the assemblage of assets - cameras, networks, databases and analytics tools - that constitute the Smart CCTV infrastructure. For example, Neighbourhood Watch could be alert for signs of suspicious activities (for e.g. drive-by hacking) in the proximity of police cameras and network infrastructure in addition to classical neighbourhood crimes.

Implementation - Other Factors

Security agencies' policies on the implementation of Smart CCTVs should factor in other critical factors; including interoperability with mission-critical systems such as criminal intelligence databases, and Command, Control and Communications systems; information-sharing between agencies; and addressing the unintended and unexpected implications such as public expectations of law enforcement standards with respect to police presence and response.

In a 2013 FBI Bulletin article on Predictive Policing: Using Technology to Reduce Crime, Santa Cruz Police Department emphasised

that technology could supplement but never supplant the innate attributes of effective law enforcement such as good investigative instincts, Humint and community engagements. Undaunted adversaries might adapt their tradecraft to outsmart electronic surveillance. For example, the Bastille Day attack in Nice occurred despite the city being known as the "CCTV capital" of France.

At present, while the AI in Smart CCTVs can highlight potential security concerns, it cannot yet perform investigative tasks like assess the intent and capability of suspects. Overreliance on technology might also affect the officers' alertness to danger and regularity of face-to-face interactions with people on the streets. Thus, an intermediate knowledge of smart technology is now critical in the skillset of officers to make them both tech and street savvy.

Smart CCTVs will henceforth have a critical role in the coming years in securing cities as well as in homeland security. Its proliferation would expectedly raise privacy concerns, and its omnipresence could inadvertently create the illusion of "gated communities" and increase complacency in terms of personal security.

Subject to a city's socio-cultural context, legislation such as the Data Protection Act in United Kingdom would help to assuage privacy concerns by regulating the responsible use of CCTVs. A healthy community partnership, such as in Singapore, would help the public to acknowledge the necessity of Smart CCTVs for the collective good and that both community vigilance and Smart CCTVs are concomitant and essential aspects of enhanced crime prevention and security strategies.

ROBOCOPS: SECURING THE CITIES OF TOMORROW

This article first appeared in RSIS commentary

Authored by
Muhammad Faizal Bin Abdul Rahman

Synopsis

Robotics offers huge potential for law enforcement in the face of new challenges and resource constraints. Nonetheless, there are organisational, operational and societal implications that the technology might bring.

Commentary

IN JULY 2016, the Dallas Police deployed a bomb disposal robot to deliver an explosive device to neutralise a shooter. The decision to weaponise a non-lethal robot was deemed necessary as other options to subdue the shooter would have resulted in more casualties. The lethal application of robots in law enforcement was reportedly unprecedented. It understandably drew profound interest not dissimilar from the military domain when such technology gained importance for offensive applications.

The operational and ethical issues stemming from the Dallas situation would be of greater relevance to countries afflicted with gun violence. For those with low crime rates, the Dallas incident presages the future of law enforcement where robots could play an integral role across the spectrum of operational functions.

Here Come Robocops

Robotics is increasingly adopted in countries which have embraced emerging technologies for smart cities initiatives, supporting a range of public-facing services including law enforcement. Research in artificial intelligence (AI) by Stanford University noted that improvements in hardware will innovate robots over the next 15 years. The World Economic Forum expects the robotics market to grow at a rate of 17% annually; and robots will be deployed in many areas of works in future.

In Singapore, robots are being piloted in various sectors; Ngee Ann Polytechnic in 2012

collaborated with the Singapore Police Force to develop a prototype Pole Climbing Robot that could deploy surveillance cameras to monitor public order situation in crowded places.

With the exponential pace of advances in AI and Internet of Things (IoT), the robots of tomorrow will be cost-efficient, functionally versatile, and capable of collaborating with human personnel. Organisations could look forward to the technology to overcome their resource constraints and enhance efficiency. Indeed, cost efficiency and functional versatility are the selling points of the latest models of security robots introduced to the market; and there will certainly be other potential benefits yet to be discovered.

The Robotic Adjutant

A feasible approach for technology adoption would be collaboration whereby robots complement human personnel in frontline duties. A paper on 'Smart Monitoring of Complex Public Scenes: Collaboration between Human Guards, Security Network and Robotic Platforms' by the US Department of Homeland Security outlines this approach. Robots interact with human personnel in performing two primary duties; patrolling for deterrence and surveillance; and gathering information on threats to support decision-making.

The designs of the latest models of robots in the market appear to affirm this approach. Chinese robotics developer Qihan unveiled 'Sanbot' which is capable of performing mobile video surveillance, interfacing with the IoT architecture, and self-recharging for 24/7 operation. American robotics developer Gamma2Robotics unveiled 'Ramsee' which is described as 'ideally suited for overnight dull, dirty and dangerous patrols nobody wants to do'.

Harnessing Robots – Issues and Challenges

Harnessing robots in law enforcement brings about challenges and issues including those which may be unintended and unexpected.

At the organisational level, human-machine interface issues need to be addressed given their complex ramifications on the human personnel's adaptation to new technology, their attitudes and productivity. A different skillset and business process reengineering would ensure proper integration of robots into the organisation.

At the operational level, an appreciation of the social context and attitudes of people when robots are present is necessary for frontline deployment of robots; lest they hamper rather than support their human partners. For example, research (i.e. "mObi" robot) in this area by New-York based Cornell University hitherto observes that robot guards have to be paired with a human for there to be any discernible deterrent effects; as long as the capability of robots is strictly surveillance rather than interventionist.

Even if the robots are unarmed or limited to non-lethal weapons, issues of supervisory and legal accountability with impact on public trust could arise if there is unexpected injury to the public resulting from non-lethal intervention (such as cardiac arrest when tasered) or technical glitches (such as driverless car accident) with the robots.

At the societal level, a calibrated implementation of robots which factors in grassroots feedback could address the concern of technology isolating the users from the community. Robots, although non-human, could in fact support community policing by enhancing service touchpoints. A precedent is the automation of neighbourhood police posts in Singapore where fully automated e-kiosks free police officers from desk duties for them to spend more time fighting crime.

The use of robots at service touchpoints however could give rise to concerns over privacy

breaches. This must be addressed from the cybersecurity and operational angles given the robots' mobile surveillance capabilities. These may be seen as more creeping compared to static CCTV cameras, and collection of personal data in its interactions with the community. The plausible risks from cyberattacks that compromise robots include personal data theft, and commandeering of the robots for launching malicious attacks and surveillance.

Additional Considerations for the Future

The nature of crime and public security will evolve as growing urbanisation introduces changes to the demography, landscape and socio-economic character of cities. Police forces will need to reshape their technical tools (such as. surveillance and community outreach) and protocols to sustain an adequate police-to-population ratio, efficient incident response, and public trust. These need to be considered as they grapple with imminent manpower constraints and new operational challenges.

Embracing robotics for staffing needs would be a strategic imperative for forward-thinking police forces as they seek to sustain their operational efficacy. While a fully autonomous 'Robocop' with a mind of its own and enforcement capabilities is likely to remain in the realm of popular culture in the foreseeable future, the role of robots in law enforcement is a certainty given the increasing pace of automation among police forces and growing pervasiveness of the technology in the public landscape.

Therefore, the evaluation of cutting edge robots and research on technical, cost and cybersecurity implications are needed. Proper integration of robots into the organisation will also require changes in organisational culture, strategies and processes. The organisational, operational and societal challenges associated with technology amid an evolving urban operating environment demand these.



IDENTITY MANAGEMENT

Law enforcement, migration and border management in an age of globalization.

Technological advancements have enabled immigration and law enforcement agencies cope with an increasingly challenging operating reality. Technology has also enabled those seeking to circumvent border controls through the use of false identities and counterfeit travel documents to facilitate illegal immigration, transnational organized crimes and/or terrorism.

Even as governments tighten immigration and border controls, there is currently no single universal standard pertaining to the identification, verification and validation of an individual's identity. These are subjected to individual countries' passport identification systems, SOPs and standards. The varying standards across the globe have resulted in gaps, which criminals and terrorists alike can exploit to commit crimes and acts of terrorism using a false or stolen identity.

The spill-over effects of this extends beyond border control challenges. Digitalisation has led to an increased use of identity-related information. Major parts of our economies and delivery of government services depend on the processing of electronic data by automated systems. Having access to identity-related information enables offenders to participate in wide areas of social life.

The abundance of personal information placed online (i.e., social media sites) has also made identity theft increasingly common and easy. Identity thefts are also conducted through phishing, data pharming and the use of spywares. The rise of identity theft made it increasingly difficult to prevent unauthorised transactions, access to information resources and installations, facilitating unlawful or cybercriminal activities across borders.



Dr Benjamin J. Muller

Associate Professor
Department of Political Science at King's
University College
President, King's University College
Faculty Association

Dr. Muller has published widely in books and academic journals on issues of borders, sovereignty, security, surveillance and biometrics, including two monographs: *Security, Risk, and the Biometric State: Governing Borders and Bodies* (Routledge 2010); and, with Samer Abboud, *Rethinking Hizballah: Legitimacy, Authority, Violence* (Ashgate 2012). Consulted as an expert witness on a number of Canadian Parliamentary committees and served as a research collaborator with NATO/European Science Foundation initiatives, Dr. Muller has also held visiting research fellowships at Western Washington University, the University of Arizona and the University of Victoria. Dr. Muller has given numerous guest lectures at Universities and Colleges in Canada and the US, as well as participated in community stakeholder initiatives on borders, security, technology, and ethics, in Canada, the US, and Europe. Dr. Muller served as the President of the International Studies Association (Canada Region 2015-2016), was a Member of the Board of Directors for the Association for Borderlands Studies (2012-2015), and currently serves as the President of the King's University College Faculty Association.

HARMONIZING GLOBAL BIOMETRIC STANDARDS? CHALLENGES AND POSSIBILITIES

*Authored by
Dr Benjamin J. Muller*

EXECUTIVE SUMMARY¹

This research begins by highlighting where biometric standards, both professional and political, currently stand. It examines important steps in the move towards wider standards for biometrics, which will enhance the interchangeability and interoperability of biometrics; and, analyzes the challenges and limitations faced by campaigns to increase standardization and the adoption and participation in these harmonization strategies globally. The report reflects on some broader challenges to biometric standardization and the general reliance on biometrics in consumer-commercial applications, national security and law enforcement. Examining the range of challenges to harmonizing biometric standards globally, such as the tensions between public government interests and priorities and those of the private biometrics industry, as well as providing action points that focus on the need to enrich and enhance the discourse on biometric technologies within the public, ideally through increased public-private cooperation. While not the panacea they were sometimes regarded to be in the immediate post-9/11 context, the effective, efficient, and secure possibilities biometrics can help bring to fruition are likely to be more palatable to all stakeholders under the conditions of governance and management that effective harmonized standards globally should provide. The need to bring critically engaging social science research on the ethical, political and legal issues associated with the applications and implications of biometrics, together with national security establishments, law enforcement agencies, and the science and technology community involved in the development of biometric technologies, is a key proposed action points with which the report concludes.

Biometrics can be useful and convenient tools for law enforcement, national security and financial security. Although convenience, efficiency, reliability and interoperability remain key benefits, the prospect of harmonized biometric standards globally remains relatively elusive. The isolationist tendencies of the US under the Trump administration, together with Brexit and the broader populist, political chauvinism this represents, suggests the global political climate is less hospitable to international regimes and resilient forms of global cooperation and coordination, of the sort necessary for the effective harmonization of global biometric standards. However, shifting the discourse about biometrics, grounded in solid research and data, might persuade citizens and their governments to advocate for certain biometrics more broadly, if effectively managed through standards and their associated organizations. Similarly, those involved in the development of biometric technologies may be convinced that the lack of harmonized global standards is hindering biometrics from becoming ubiquitous, which could prove to be an acceptable trade-off for the alleged “costs” associated with standardization, such as “patent ambush” and restrained innovation. Although creating more resilient international standards and their respective institutions is a worthwhile cause, concentrating efforts on citizens, governments, and the biometrics industry itself, is likely to yield more success. The lack of robust, harmonized biometric standards globally has much to do with skeptical and critical publics, transient and impatient governments, and elusive market actors who often believe “industry standards” to be sufficient.² Engaging these stakeholders effectively to develop harmonized biometric standards globally has the potential to

foster technological innovation, quell many legitimate concerns with biometrics – such as the transfer of personal data between states and public and private actors without sufficient oversight, and deeper and more complex issues associated with “social sorting”³ and the stratification of identities into various categories of suspicion – and provide enhanced management and opportunities for use.

Although biometric standards go back as far as 1986 (ANSI/NBS-ICST 1-1986),⁴ due in part to the increased use of biometrics by national security agencies and law enforcement since 11 September 2001, biometric standards increased throughout the first 15 years of the 21st century (BioAPI 2001, 2002, 2006).⁵ As industry experts note, while the existence and maturity of standards have increased in the past decade, adoption and participation in these standards from a broader cross section of users continues to lag.⁶ Moreover, as experts like Tilton provide a sound account of the evolution and current status of biometric standards, as well as the relevant national and international organizations involved in the development of these standards, such accounts remain thin in terms of their deeper, critical analysis. It is worth noting that the sort of global harmonization that may be the subject of fantasy of national security agencies, financial institutions and law enforcement, seems to imagine an international regime with a robust architecture which is almost non-existent throughout global politics, and if anything, is currently under serious threat. While the international passport regime is among the most robust of global regimes, even the International Civil Aviation Organization (ICAO) finds itself hindered by differing legal, ethical and socio-political norms across national jurisdictions, not to mention vast disparities among bureaucratic and governmental capacity to implement biometric strategies.⁷

Developing harmonized biometric standards globally faces a series of key challenges. The tensions between the public/state use of biometrics for national security (borders, visas, immigration, passports, etc.) and the private/commercial use (credit cards, payment and logistics systems, etc.) is often characterized by divergent interests when it comes to a harmonized standard. Related to this, the frenetic pace of technological innovation in biometrics poses its own challenges, as does the alleged negative impact of standardization on this innovation. Furthermore, the related inability to marshal the necessary ethical, legal and political tools to manage the applications and implications of these technologies (thus, convincing skeptical citizens),⁸ as well as accompanying harmonization of standards. Finally, different legal-political jurisdictions in which biometrics might be used for law enforcement, border security management, and commercial exchange.

Unpacking the contemporary landscape of biometric standards, as well as the diverse and complex challenges faced by efforts to harmonize biometric standards globally, allows one to critically assess the success and failures in the story of global biometric standards. Both the European Union and North America provide productive sites for analysis of relative success stories. Diverse political cultures, and differing ethical and legal contexts have in many cases been negotiated successfully, advancing biometric standards and relatively robust bilateral and multilateral architectures for their use. Complimentary biometric entry-exit visa systems in Canada and the US, fostered by a range of bilateral agreements, not least the *Beyond the Border Action Plan*,⁹ have enhanced capacity and cooperation among law enforcement and negotiated divergent political cultures and legal traditions. Similarly, the entire Schengen architecture

in the European Union relies heavily on biometric technology and data-sharing, while negotiating sound data-protection and privacy legislation across an incredibly diverse range of legal traditions, ethical contexts, and political cultures. Moreover, in both the EU and North America, technological innovation in biometrics has flourished, as has staunch engagement in the formal and informal bodies charged with developing harmonized biometric standards.

It is clear, as a former Canadian Minister of Citizenship and Immigration noted in 2003, “the biometrics train has left the station.”¹⁰ Harmonized global standards for biometrics are an essential next step to take this technology from a “boutique” style of competitive advantage to an interoperable system for enhanced national security, financial security, and law enforcement. However, how do we get from here to there? The research report lays out a range of challenges and action points, not least of which is the tension between public and private interests on this matter. Bringing together critical social science and humanities scholarship to the table is essential to take seriously the ethical, political and legal challenges posed by the applications and implications of biometrics. This will serve to erode the divisions between public, governmental interests in national security and law enforcement, and private interests for competitive advantage compelled by free market ideals. The lineage of biometrics and related technologies associated with its genesis, such as fingerprinting and DNA analysis, have spotted histories of sometimes problematic categorizations on the basis of race, class and gender, which is well documented.¹¹ Together with ongoing revelations from both Edward Snowden and Wikileaks, suspicious and skeptical citizens and corporations need assurance that the step towards globally harmonized

standards for biometrics will also enhance privacy and robust forms of independent oversight. Framing the moves towards global standards in this manner, will not only enhance the possibility for essential public “buy-in,” but also contribute to assuage the suspicions from private industry that these steps towards global harmonized standards undermine competitive advantage and innovation.

REFERENCES:

Bennett, Colin J., and David Lyon. “Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.” Text. Routledge.com, 2009. <https://www.routledge.com/Playing-the-Identity-Card-Surveillance-Security-and-Identification-in-Bennett-Lyon/p/book/9780415465649>.

“Beyond the Border Action Plan,” June 28, 2016. <https://www.publicsafety.gc.ca/cnt/brdr-strtg/bynd-th-brdr/ctn-pln-en.aspx>.

Calo, Ryan. “Privacy and Markets: A Love Story.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, August 6, 2015. <https://papers.ssrn.com/abstract=2640607>.

Cole, Simon A. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, Massachusetts: Harvard University Press, 2002. <http://www.hup.harvard.edu/catalog.php?isbn=9780674010024>.

Lynch, Michael, Simon A. Cole, Ruth McNally, and Kathleen Jordan. *Truth Machine: The Contentious History of DNA Fingerprinting*. University of Chicago Press, 2010.

Lyon, David. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Psychology Press, 2003.

Magnet, Shoshana. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press, 2011.

Muller, Benjamin. "Borders, Bodies and Biometrics: Towards Identity Management." In *Global Surveillance and Policing*, edited by Mark B. Salter and Elia Zureik, 83–96. Willan Publishing, 2005.

Pugliese, Joseph. *Biometrics: Bodies, Technologies, Biopolitics*. Routledge, 2012.

Tilton, Catherine J. "Biometric Data Complies with Impending Privacy Legislation." *Planet Biometrics*. Accessed May 17, 2017. <http://www.planetbiometrics.com/article-details/i/5574/>.

———. "Microsoft Word - Biometric Standards White Paper_March2009 - Biometric_Standards_White_Paper_March2009.pdf," March 2009. http://www.nws-sa.com/biometrics/Biometric_Standards_White_Paper_March2009.pdf.

Tilton, Catherine J., and Matthew Young. "Standards for Biometric Data Protection." In *Security and Privacy in Biometrics*, edited by Patrizio Campisi, 297–310. London: Springer London, 2013. http://dx.doi.org/10.1007/978-1-4471-5230-9_12.

Wilcox, Lauren B. *Bodies of Violence: Theorizing Embodied Subjects in International Relations*. Oxford University Press, 2015.

⁴ Catherine J. Tilton, "Biometric Standards White Paper_March2009 - Biometric_Standards_White_Paper_March2009.pdf," March 2009, http://www.nws-sa.com/biometrics/Biometric_Standards_White_Paper_March2009.pdf.

⁵ Catherine J. Tilton, "Biometric Data Complies with Impending Privacy Legislation | Planet Biometrics News," accessed May 17, 2017, <http://www.planetbiometrics.com/article-details/i/5574/>; Catherine J. Tilton and Matthew Young, "Standards for Biometric Data Protection," in *Security and Privacy in Biometrics*, ed. Patrizio Campisi (London: Springer London, 2013), 297–310, http://dx.doi.org/10.1007/978-1-4471-5230-9_12.

⁶ Tilton, "Biometric Data Complies with Impending Privacy Legislation | Planet Biometrics News."

⁷ Colin J. Bennett and David Lyon, "Playing the Identity Card: Surveillance, Security and Identification in Global Perspective," Text, Routledge.com, (2009), <https://www.routledge.com/Playing-the-Identity-Card-Surveillance-Security-and-Identification-in/Bennett-Lyon/p/book/9780415465649>.

⁸ Joseph Pugliese, *Biometrics: Bodies, Technologies, Biopolitics* (Routledge, 2012); Simon A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press, 2002), <http://www.hup.harvard.edu/catalog.php?isbn=9780674010024>; Shoshana Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham: Duke University Press, 2011).

⁹ "Beyond the Border Action Plan," June 28, 2016, <https://www.publicsafety.gc.ca/cnt/brdr-strtg/bynd-th-brdr/ctn-pln-en.aspx>.

¹⁰ Benjamin Muller, "Borders, Bodies and Biometrics: Towards Identity Management," in *Global Surveillance and Policing*, ed. Mark B. Salter and Elia Zureik (Willan Publishing, 2005), 83–96.

¹¹ Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification*; Michael Lynch et al., *Truth Machine: The Contentious History of DNA Fingerprinting* (University of Chicago Press, 2010); Pugliese, *Biometrics*; Lauren B. Wilcox, *Bodies of Violence: Theorizing Embodied Subjects in International Relations* (Oxford University Press, 2015).

¹ Special thanks to the instructive comments and edits on earlier drafts of this summary from Damien Dominic and Samer Abboud. Also, thanks for research support from Simon Stan and King's University College at Western University.

² Ryan Calo, "Privacy and Markets: A Love Story," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, August 6, 2015), <https://papers.ssrn.com/abstract=2640607>.

³ David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Psychology Press, 2003).

**Augustine Chiew**

Global Public Safety Expert
Enterprise Business Group
Huawei Technologies Co., Ltd

A Global Public Safety Expert in Huawei, Augustine focuses on helping governments and public agencies better understand public safety challenges and emerging trends to identify solution requirements. He works closely with the Huawei product and solution team to develop lead ICT solutions for policing and border management taking into consideration public safety best practices.

Augustine has more than 20 years of public safety experience. He was with the Singapore Police Force and the Singapore Ministry of Home Affairs for 17 years and held various appointments in Operations, Homefront Security, Planning and International Partnerships. He also worked as a consulting Executive focused on public safety in a leading global firm that provides strategy, consulting, digital, technology and operations services for 3.5 years.

An advocator of collaborative policing, Augustine was active in international policing and served as the Chairman of the INTERPOL Working Group on Cybercrime (2012-13). He has a Bachelor of Business Studies from the Nanyang Technological University (NTU).

CLOUD ENABLED DIGITAL IDENTITY MANAGEMENT

*Authored by
Augustine Chiew*

Age of Digital Identity

We now live in an era where people are more connected than ever. Information exists in multiple forms and formats, collected and made available across multiple channels. Our personal Identification Data (IDs) no longer differentiates or identifies who we are but is also used to perform a huge variety of everyday transactions linked closely to the way society operates. It is no longer a choice of how we want to live but rather how much we need to embrace it to pursue a meaningful life.

As we shift more and more towards the era of Digital Identity where identities may no longer be fully established given the information overload, it is increasingly clear that well-defined processes that have served governments and businesses so well in the past may no longer hold the key towards identifying an individual absolutely, uniquely and definitively in any scenario or circumstance. ID management processes will likely need to access all sources of available information and combine it with prior data that has been collected and enrolled in existing databases to make informed opinions about the identity of an individual. These trends suggest that we will need to manage and live with errors and somehow strike a good balance between security and efficiency.

Driving Forces shaping the future

The UN and World Bank ID4D initiatives have set a goal of providing everyone on the planet with a legal ID by 2030. To that end, numerous new national eID programs (including card and/or mobile-based schemes) have been launched or initiated. New standards driven by ICAO, NIST and IATA have also emerged, fostering compatibility and interoperability. Innovative technologies and regulations have also been used extensively to support and

shape the digital transformation ahead. Some examples include:

- Digital Driver's Licence in UK, USA, Australia and the Netherlands
- E-residency programmes in Estonia and UK
- Smart Borders/Airports in many countries worldwide
- The European Union's Electronic Identification and Signature (eIDAS) regulation that came into force in July 2016

Moving forward, we expect these initiatives and programmes to gather more and more momentum underpinned by key driving forces that will shape Digital Identities over the next 1-3 years:

- Domination of mobile communication as the key platform for accessing services, both government and businesses, will continue to drive the development of mobile-first solutions
- Greater and growing balance between Trust and Privacy as citizens embrace the need for enhanced robust security measures in digital transactions. There are clear signs that citizens are willing and prepared to sacrifice some data privacy paving the way for the creation of a Public Framework of Trust
- Evolution towards Smart Cities as mass populations move to urban environments at an increasing pace. Inevitably, technological developments will be inextricably linked with this mass migration as citizens look towards more eGovernment or mGovernment services that can be accessed on demand. Smart Cities will be the new playground in this century we live in
- Maturity of digital identity standards and technologies as more and more countries display a greater willingness to come forward and work together to set

internationally recognized standards as well as rapid movement from proof-of-concept technologies to applicable solutions

- Increased government recognition of the need and ownership of ID programmes as they support and coordinate local government investments through which local transformations, close to the community, can operate effectively and efficiently

Evolving Threats & Challenges

All these developments suggest that the amount of data needed to build a profile of a person will grow exponentially. The data will exist in multiple forms, across multiple channels, and would have to be collected over an extended period of time, possibly across an entire lifespan. Hence, there will be huge storage and cost challenges. At the same time, fierce competition for ICT talent means that many organizations are unlikely to have the right resources to be able to implement and maintain the necessary infrastructures needed.

ID management is expected to be integrated more and more into complex business processes operated in parallel by multiple agencies, whether they are public, private, national or international. Hence, many agencies will need to have access to the complete identity chain, although they only own and have access to partial information. Without cooperation and collaboration, especially in terms of data/information sharing, it would be almost impossible to operate effectively and efficiently. At the same time, there is the need to strike a balance between data sovereignty and access control to protect data privacy.

Rising citizens expectations, the need to operate economies and businesses optimally, means that high computing power is needed to sieve through structured, semi-structured and unstructured data quickly to meet real-time mass processing needs. After all, it is

inconceivable to expect e-transactions to take more than a couple of seconds in this digital era where speed is paramount.

Cloud Computing - The Path Forward

Cloud Computing will light the path moving forward. In simplistic terms, it is the delivery of computing services—servers, storage, databases, networking, software, analytics and more, over the Internet. When applied to public safety IT systems, such as Identity Management, the architectural characteristics of Cloud Computing will strengthen related agencies' ability to manage threats and challenges effectively and efficiently, while optimizing scarce resources. It is a shift from the traditional way of viewing how IT resources should be procured, managed and used. Some of the key benefits of Cloud Computing are:

- It cuts costs by eliminating capital and operating expenditures such as hardware and software procurement, setting up and running physical on-site data centers, related power and cooling expenses, salaries of IT team, and so on
- Provision of services on demand with glitches easily managed within minutes, giving users lots of flexibility and taking the pressure off capacity planning in the process
- Eliminates time-consuming IT-related administrative chores such as “racking and stacking” and software patching so clients can operate on leaner IT teams that spend time on important business goals
- High computing power through regular upgrades to the latest generation of fast and efficient computing hardware, which are secure, thereby achieving greater economies of scale
- The ability to scale elastically by delivering the right amount of IT resources such as computing power, storage, bandwidth at the right time in the right geographic location

- Data backup, disaster recovery and business continuity made easier and less expensive as data can be mirrored at multiple redundant sites

Why Huawei?

In this regard, Huawei has developed a comprehensive set of Cloud Computing solutions complemented by Big Data to support Identity Management.

FusionSphere, Huawei's Distributed Cloud Data Center (DCC) operating system is able to meet the evolving and unpredictable demands of public safety, including identity management. Using Software-Defined Networking (SDN), these platforms implement a virtual data center that supports automated management of physically scattered resources achieving optimization.

As it is based on OpenStack, FusionSphere also enables the unified management of virtualized resource pools, physical servers, storage equipment, and networks that may be deployed based on demand. By providing services and functions through Virtual Machines, Huawei is able to eliminate the high expenses associated with dedicated hardware, deliver identical services at a fraction of a cost allowing greater value for money. Load-balancing functionality assures efficient and optimal utilization of CPU and memory resources with fast failover when faults occur. This is extremely crucial given that borders are more often than not, our first and last line of defence against crime and terrorism.

Within the Huawei Cloud solution, a customized Hadoop platform is used to host Big Data processes that include data query, data mining, analytics, and real-time streams of structured, semi-structured and unstructured data. This enables rapid mass data processing and analysis, allowing queries

to be addressed quickly while strengthening insight driven decision make.

In addition, Huawei's ManageOne will simplify the Operations & Management (O&M) of Software defined Data Centers (SDDCs) by integrating SDN with Software Defined Storage (SDS). This is crucial as many public safety agencies and their sub-units have their own data centers that were procured together with business solutions and systems. Given they were bought during different time periods and are designed to operate independently, many cannot be integrated easily to support information sharing, which is an integral part of identity management.

Huawei is able to manage these data centers that are likely to be located at multiple locations in a unified and efficient manner to support a broad range of services needed. Through virtualization, these data centers can be divided into as many Virtual Data Centers (VDCs) as needed to support multiple Virtual Private Clouds (VPCs) with each supporting different public agencies' services and operations.

Conclusion

In time, Digital ID infrastructures will replace paper-based processes and allow agencies charged with Identity Management the ability to align their operational efficiencies. Through Cloud enabled platforms solutions, we can manage the challenges arising from growing citizen expectations, the dynamic ever changing digital identity and a global population reliant on mobility.

**Michael O'Connell**

Director for Operational Police Support
and Analysis
INTERPOL

Michael O'Connell is the Director for Operational Police Support and Analysis at INTERPOL, Lyon, France. Responsible for both strategic and operational activities, he commands a diverse directorate that includes police forensics, police information management, crime analysis, fugitives, border security, 24/7 operational and crisis/major incident support capabilities.

He has led a variety of innovative projects including the creation of INTERPOL's Integrated Border Management Task Force, delivering operational response to border security threats, capacity building programmes that lead into successful field operations tackling human smuggling, counter terrorism, narcotics, firearms trafficking and major international event security; I-Checkit – developing robust and assured public private partnerships to protect and detect threat in the aviation, maritime and our global mega/smart city environs; Project STADIA – delivering capacity building to the State of Qatar for their FIFA World Cup in 2022, and hosts of other major international events.

Michael started his policing career in the Metropolitan Police Service, specialising in major crime and covert policing operations against trans-national crime threats, having worked in most continents. He has since gone on to serve terms with the National Crime Squad of England and Wales, The Serious Organized Crime Agency (SOCA), and is now a serving officer with the National Crime Agency (NCA, UK).

He is a graduate of the Metropolitan Police Training Academy and other UK national crime agencies in Detective, Covert Policing and Senior Investigating Officer programmes. He has successfully completed the Top European Senior Police Officers Course (TOPSPOC), has professional management qualification from the UK Open University, has written and published a variety of papers on International Policing topics, and a graduate of the Executive Leadership Program with the Australian Institute of Police Management (AIPM).

DARE TO SHARE: THE VALUE OF PUBLIC-PRIVATE PARTNERSHIPS

*Authored by
Michael O'Connell*

Every day, our international borders are confronted with over eight million passenger movements, which equates to a 'floating' population in the skies in excess of one million people at any given minute. International arrivals have exploded from 25 million in the 1950s to 1.2 billion in 2015, to a projected two billion by 2030. This unprecedented growth is placing our public sector guardians of borders under intolerable pressure to fulfill their primary responsibility: to protect. This dramatic growth has also led us into a situation some would describe as chaotic, exposing risk that requires new thinking to mitigate, and hence presents an opportunity for change: partnering with the private sector.

The public sector is a cautious beast, especially when we consider its role in ensuring public safety and security. Its mandate in this regard is further complicated when matters of national security - including protecting its borders - are taken into consideration, leading to heavy regulation, cautious officials, a 'suspicious by design' approach, and acute information security protocols in relation to identity management.

This leads to an operating environment which is complex, multidimensional, bureaucratic, inflexible and often overwhelmed by demand. An environment which is further compromised when subject to sustained financial challenge for increased efficiency gains and resource reductions to meet a variety of public finance imperatives, leading to pressure points that can and often do expose borders to risk in particular.

Now, add globalization to this environment and the necessity to develop a complimentary global architecture of standards, technology, identification management, legislative

frameworks, systems and processes. These must respond to all national administrations and international bodies, but in a way that is permissive to trade, commerce, and regularized travel, with a seamless interface to the private sector.

Yes, you would be right to think it could lead to a situation of unimaginable chaos. Thankfully, it is not as bleak a picture as we might believe, due in no small part to the opportunity for change.

At INTERPOL, we have the privilege to support 190 member countries in their desire to better police and protect their citizens, and especially their borders, and by default enhance their national security resilience. As you may expect, this membership presents itself at a variety of levels of development, sophistication, and tolerance to the global pressures of international travel. Yet, they all have a common need: to protect. It is the role and responsibility of INTERPOL to innovate and support them in this task.

The police and border security community, generally a body of public security professionals, and typically 'suspicious by design', have an ingrained intolerance to sharing information, particularly with the private sector. Yet, they are at the heart of the change imperative. Whilst it is interesting to see some sectors of exception, with cybersecurity developing itself as a leader in change, border security remains an area of acute sensitivity. As a general rule, these officials are happy to receive information, but unwilling to share.

The experience of border security professionals at INTERPOL led us to believe that to overcome some of these restrictions,

we would have to enable cultural change by 'daring to share' with the private sector. The innovator we used for this was I-Checkit, a tool which would build trusted partnerships between the public and private sectors with a primary aim: to protect.

What is I-Checkit?

I-Checkit is a screening service that complements and enhances existing national border security systems. It allows trusted private sector partners to conduct advanced passenger checks in real-time, in collaboration with the global law enforcement community.

Currently, I-Checkit is operational in the travel industry, with airlines and, more recently, cruise lines. I-Checkit enables carriers to submit passengers' travel document information for screening against INTERPOL's Stolen or Lost Travel Documents database (SLTD).

A database match triggers an instant alert so the situation can be investigated. These alerts are sent to the INTERPOL General Secretariat's Command and Coordination Centre, INTERPOL National Central Bureaus in the countries concerned, and other relevant national law enforcement entities. In some cases, they are also sent to carriers' security teams to enable them to carry out a physical check of the document in question at the boarding gate.

Why I-Checkit?

Experience has shown the international law enforcement community that, as travel documents become more sophisticated and harder to duplicate, criminals often rely on stolen and altered identity documents to move across borders, open bank accounts, purchase plane tickets and check in to hotels. Fraudulent travel documents can therefore be used to perpetrate serious crimes such as money laundering, human trafficking and terrorist activities.

The United Nations Security Council Resolution (UNSCR) 1617 of 2005 recognized this reality by urging countries 'to ensure that stolen and lost passports or other travel documents are invalidated as soon as possible and share information on those documents with other member states through the INTERPOL Stolen and Lost Travel Documents (SLTD) database'.

Since its creation in 2002, the SLTD database has become one of INTERPOL's most used and valued tools for member countries. It now contains more than 70 million records from 174 countries and was searched more than 1.7 billion times in 2016. It has been endorsed by international organizations including the G8, the Asia Pacific Economic Cooperation (APEC), the European Union (EU) and the International Civil Aviation Organization (ICAO).

In 2009, INTERPOL created a Travel Documents Associated with Notices (TDAWN) database subset. TDAWN contains genuine travel documents belonging to known criminals, and helps identify wanted criminals subject to INTERPOL notices when checking their travel documents.

Despite these valuable police resources, there is still a significant security gap to be filled when it comes to the movement of people - a gap which is expected to grow as more people undertake transnational travel. The dramatic increase in travellers will put an even greater burden on countries that do not have the resources to screen every person who enters their territory. Indeed, very few countries have the mechanisms in place to screen passengers leaving their territory or travelling within it. Moreover, many borders are becoming increasingly permeable to facilitate international travel.

If no additional controls are put in place and the number of international travellers increases as expected, the amount of unscreened passengers will continue to grow. As we know, it only takes one successful criminal or terrorist to jeopardize the safety of the public at large.

So How do you Convince the Inconvincible?

You develop a blueprint for public-private partnerships that is trusted and assured for global use. It must have the confidence of the public sector and its security authorities through an accredited secure network of private sector professionals.

Create a Solution that is Secure by Design

At its heart, we had to create a solution that was universally accepted, global in design for interfacing with up to 190 countries, providing ease for interconnectivity with the private sector, in addition to delivering trusted systematic security accreditation and assurance to each member state and their data protection bodies.

Build a Robust Legislative Framework

With the primary aim of delivering safer borders through lawful and proportionate exchange of passenger information, we were able to develop a system working to the highest international standards through a legislative framework that respects personal privacy, national legislation and industry norms for the safe and effective operation of air carriers and the maritime sector.

This entailed not just legal qualification against the robust information exchange processes that hold INTERPOL activity to account (the INTERPOL Constitution and the Rules for the Processing of Data), but also each participating member country and their data custodians (DPO officers).

Ensure the Innovative Use of Technology

At the heart of I-Checkit was 'security by design' and an imperative to ensure low-cost connectivity to industry. To achieve this, we chose to base its development on an existing tested INTERPOL interface which we outsourced to the private sector in order to create a 'next-generation' solution. The result was a robust tool that could embrace and assure a public-private data network for the exchange of sensitive border security information.

To further ease the diverse client needs between the public and private sectors, we also had to ensure maximum flexibility on system functionality. This required the development of a multi-dimensional information management strategy that was responsive to need. This allowed strict data visibility rules, access, storage, transmission and use through a three step model of 'visible', 'blind' and 'opt-out'.

It also had to tolerate extremes in volume, as more than 70 million records are held within INTERPOL's SLTD database. With these records used as the primary tool to identify risk, we had to ensure they could be screened against ever-expanding international passenger movement figures in the billions.

Build Trusted Partnerships

To develop a 'trusted partnership' status, we sought to build assured partnerships through a robust access and accreditation framework that permitted proportionate data exchange, with a purpose to achieve regulated security benefits.

Aim to Deliver Operational Success

The overriding principle of I-Checkit was the need to deliver tangible operational success. INTERPOL now offers a solution that can detect transnational criminals and terror threats to permit lawful intervention and risk mitigation. It interacts with a large number of stakeholders such as governments, regulatory

bodies, the travel industry, professional associations and technology services partners in the private sector, and its value can be demonstrated in the following ways:

1. I-Checkit provides early identifiers and alerts law enforcement and carriers about passengers travelling on lost or stolen documents and, soon, those identified as a criminal or terrorist threat through the 'TDAWN' solution.
2. I-Checkit enables member countries that do not have integrated border solutions to increase screening against INTERPOL's databases through the private sector, permitting advance detection and deterrence of identity fraud, illicit cross-border movement and associated terrorist and criminal threats.
3. I-Checkit is well-positioned to effectively respond to UNSCR 2178 concerning foreign terrorist fighters (FTFs) and it is compliant with UNSCR 2309 to ensure the safety of global air services and prevent terrorist attacks to civil aviation.
4. For airlines, I-Checkit mitigates the risks associated with repatriation costs for

passengers travelling with stolen or lost travel documents. Hence, it improves the chances of compliance with national legislation and may help reduce financial liabilities resulting from non-compliance and security breaches. It can assist in ensuring that flight operations remain optimized by limiting disruptions to departures associated with undocumented or illegal travellers.

5. Simple and cost effective means to improve customer due diligence – the Know Your Customer, or KYC approach.
6. For the private sector, a partnership with INTERPOL is likely to be perceived favourably by customers and may positively impact companies' operations, image and reputation.

To date, I-Checkit has succeeded in demonstrating its value. With over 82 million screenings and almost 2,300 positive hits since June 2014, the I-Checkit solution was INTERPOL's 11th highest user of SLTD searches in 2016 – ahead of most INTERPOL member countries. Below are I-Checkit's key statistics for the aviation sector and two success stories which illustrate how it supports existing border security systems:





In conclusion, the future might not be as daunting as we expect, if we are willing to innovate and seize the opportunity to change by daring to share for mutual benefit through public-private partnerships. We can succeed,

as we have proven at INTERPOL with I-Checkit. Looking at it from the perspective of Sun Tzu, one might say we have 'snatched opportunity from the jaws of chaos'!

**Derek Pak**

Vice President, Franchise Integrity
Mastercard

Derek Pak has spent a total of over 30 years in law enforcement and fraud risk management. He began his career with the Singapore Police Force after graduating from the National University of Singapore. Following his law enforcement stint, Derek joined the banking industry and distinguished himself as a fraud risk management professional, firstly with Citibank as the Regional Head of Fraud Risk Management and subsequently with Standard Chartered Bank as the Head of Fraud Risk Management Strategy for Channels and Products. Most recently, Derek joined Mastercard as the Regional Lead for Customer Fraud Management covering the Asia Pacific region.

Derek is well versed in dealing with the continuously evolving fraud and business challenges the payments industry face. He thrives on finding innovative solutions with optimal balance between controls and cardholders' experience to mitigate risks.

SECURING THE EVOLVING PAYMENTS WORLD

*Authored by
Derek Pak*

As the digital economy continues developing, change is its only constant. We see consumers shift from being PC-first to mobile-first users, with a significant amount of time spent on their mobile devices. They want to be able to use their devices anytime, anywhere and for a multitude of purposes such as booking a cab, finding the fastest route, transferring funds, purchasing movie tickets, securing cheap flight tickets, and ordering their food ahead of time. The list is endless, and the underlying behavioral shift can be attributed to the increasing desire for a seamless and secure consumer experience in their everyday life.

Likewise, anti-fraud technologies in the payments industry must also evolve with the changing landscape. To protect against all forms of card fraud, organizations must take a multi-layered approach to securing payments. Various solutions, from EMV and tokenization to biometric authentication and artificial intelligence capabilities, are required to protect card-present and card-not-present transactions from different fraud modus operandi. These technologies help to detect and prevent fraud, reduce false declines, enhance consumer experience and cut operational costs, benefiting all stakeholders except, of course, the fraudsters.

EMV Chip

Much has been said about EMV chip cards; they provide substantial protection for card-present transactions against counterfeiting. As one of the founders and first adopters of EMV technology, Mastercard has been a primary driver behind the significant strides that EMV technology has made in addressing fraud in regions with chip-based payment transactions. Besides exceeding expectations in reducing counterfeit fraud, EMV has increased operational efficiencies,

improved offline risk management, and a host of enhanced value-added solutions that go beyond simply making transactions more secure for cardholders.

As the adoption of EMV technology becomes increasingly widespread, the entire payment card ecosystem continues to reap benefits. Mastercard remains committed to working with key players in the payments ecosystem in building new EMV roadmaps and enhancing existing ones to ensure that key learnings and best practices for migration are best applied.

Tokenization

There is a strong need to minimize unauthorized use of card account data and to reduce cross-channel fraud for card-not-present transactions which combine elements of card-present and card-not-present transactions. Mastercard seeks to enable every device to be a commerce device and thus, have developed solutions that promise to enable digital payments across a wide spectrum of transaction types. These include payments initiated through digital wallets and near-field communication (NFC)-enabled devices such as smartphones, tablets, and “in-app” payments. Among the solutions are Payment Tokens that are designed to replace a card’s primary account number (PAN) with a surrogate value. This substitution provides an additional layer of security that eliminates the need for merchants, digital wallet operators (DWOs), and other transaction participants to store real account numbers.

Mobile payments are a primary contributor to this evolution as well as the progressive convergence between the physical and digital worlds. In fact, this convergence has altered the way consumers shop at physical and virtual merchant locations, as the nature of

the interaction moves away from traditional plastic cards to payments-enabled Internet-connected devices and other forms of digital payment.

Biometric Card

Mastercard has introduced the next generation biometric card, combining chip technology with fingerprints to authenticate the cardholder's identity for card-present transactions. The card, which builds on the fingerprint technology used in mobile wallets, can be used worldwide at any Point-of-Sales equipped with EMV terminals as it works like any other chip card. The EMV card terminal infrastructure does not require any hardware or software upgrade. During registration with the issuing bank, the cardholder's fingerprint is converted into encrypted digital template and stored on the card. During payment, the cardholder simply inserts the biometric card into the EMV terminal while placing the finger on the card's embedded sensor. The fingerprint is verified against the digital template and, if it matches, is approved without the card ever leaving the cardholder's hand.

Identity Check Mobile

Forgetting passwords is a frequent point of friction in payments, and our studies have shown that a majority of consumers want to see passwords replaced by something more convenient without compromising on security. Given the proliferation of smartphones with high-resolution cameras and fingerprint scanning technology, biometric authentication is fast becoming commonplace. Riding on these technologies, Mastercard's Identity Check Mobile application offers additional and alternative forms of authentication via fingerprint and facial recognition to make payment transactions seamless and more secure.

Decision Intelligence

Fraud technology is not just about biometrics.

With Decision Intelligence, Mastercard uses Artificial Intelligence and machine learning capabilities to reduce friction and fraud. The algorithms crunch transactional data and complex behavioral data to make decisions in nanoseconds. Decision Intelligence is a radical new approach that goes much further than current fraud scoring methods to detect normal and abnormal spending behaviors. It takes a broader view in assessing, scoring and learning from each transaction. That score comprises account information like customer value segmentation, risk profiling, location, merchant, device data, time of day, and type of purchase made, enabling the card issuer to apply the intelligence in real-time or to the next transaction. This allows them to react to potential threats much quicker, thereby reducing operational expenses like chargebacks.

The key objective of Decision Intelligence is to minimize false declines which consumers dislike as they want all their payments to go through and be approved without any friction. This technology keeps learning and enables itself to make smarter decisions over time, helping to reduce fraud perpetrated by criminals and increase seamless transactions for the consumers.

Mastercard Safety Net

Criminals are continually developing new and sophisticated tools and techniques to compromise account data and breach security defenses. As fraud techniques rapidly evolve and spread across countries and regions, organizations need to keep up or risk suffering catastrophic losses.

Mastercard Safety Net acts as an external layer of security complementing the issuer's own defenses to limit the impact of a large-scale fraud attack on one or more of their payment channels (e.g. ATM, e-commerce). The service can also identify largescale fraud attacks in

real-time, utilize insights from the Mastercard Network and provide protective measures, so that appropriate action can be taken by the issuer. It does not replace an issuer's primary fraud prevention system.

Mastercard Forensic Reader

Notwithstanding the numerous technologies developed to prevent fraud and detect fraud when it happens, fraudsters will always find ways to perpetrate their illegal activities. This is why Mastercard developed a solution to help law enforcement agencies (LEA) with their investigations when fraudsters are arrested and found to be in possession of suspected counterfeit or stolen cards. The Mastercard Forensic Reader (MFR) is the first device in the world to accurately detect payment card fraud within 20 seconds.

The MFR, which resembles a typical Point-of-Sale terminal, helps to improve the effectiveness, timeliness and accuracy of investigation as it allows LEA agents to quickly process the seized cards to verify its authenticity in a situation where time is of the essence. If the cards are determined to be fraudulent, the agents will be able to expeditiously contact the impacted issuer using the contact information provided by the MFR.

Conclusion

Keeping ahead of increasingly sophisticated criminal networks is a challenge, and there is no silver bullet to preventing fraud. However, it's important that the responsibility of ensuring the safety and security of payments is shared by both issuers, merchants and cardholders.

Securing payments requires industry-wide collaboration to enable a seamless and secure experience throughout the entire payments ecosystem. Players in the global payment space must come together to share insights,

solutions and best practices to deliver the highest levels of security, while better enabling the consumer to pay conveniently.

Simultaneously, the industry needs to continually work together to build trust in digital and mobile payment technologies. Education is paramount to instilling confidence in consumers, regardless of their demographic or spending power, and to ensure making safe and secure payments remains a key priority for all.

**Dr Guy Vinet**

Head of Strategic Police Matters Unit /
Transnational Threats Department
Organization for Security and
Co-operation in Europe (OSCE)

Guy Vinet is the Head of the Strategic Police Matters Unit of the Transnational Threats Department of the OSCE Secretariat. He is a colonel (rtd) of the French Gendarmerie. He has worked extensively in South-Eastern Europe for the UN, NATO and the European Union. He has supervised police operations in Africa and French overseas territories. He is a graduate of the Air Force Academy, the National Gendarmerie Academy, and the Army Senior Staff College. For two and half years before joining the OSCE Secretariat, he supervised the Security Cooperation Department at the OSCE Presence in Albania. Mr Vinet holds a PhD in Political Science and Masters' degrees in International Relations, Geopolitics and Diplomacy from Paris Universities.

LAW ENFORCEMENT, MIGRATION AND BORDER MANAGEMENT IN AN AGE OF GLOBALIZATION

*Authored by
Dr Guy Vinet*

“Know the enemy, and know yourself, and you will never be in peril”, Sun Tzu¹, 500 BC

From a law enforcement perspective, there is nothing more relevant than that. And the enemy we face here is crime. Since more than 2500 years, these principles have not changed.

Indeed, there is nothing new under the sun; however everything is new!

There is nothing new in the sense that crime is as old as mankind. For centuries/mellennium we have always had people trying to do something wrong to others or something that contravenes the rules.

However, we are now in the time of so-called globalization, and some things have changed in the state of the affairs of law enforcement.

Organized crime was invented when two persons agreed to defraud, steal from or kill a third one, some time ago. Pirates who looted commercial vessels in the 17th century and who undertook the large-scale trade of stolen goods may be considered among the earliest organized crime groups. It became a more notorious reality in the early 1800s in Italy and the United States of America, when the first very structured criminal groups took action. These were followed by mafia-type groups on all continents. Today, organized crime has an internationally recognized definition and transnational organized crime is subject to a United Nations Convention (UNTOC).

Terrorism had already affected France by the late 18th century, when the word itself appeared for the first time, while the United Kingdom and Russia starting being affected in the late 19th century. In the USA, President

William McKinley was assassinated in 1901 by an anarchist. In reality, terrorism is as ancient as political conflicts and warfare between human groups (Sicarii, Assassins, Mongols and Tamerlane, to name a few examples). I will not get into the argument of defining terrorism because, as you know, no definition is legally and universally recognized.

Terrorism is a tool, or a technique, and from a law enforcement perspective it is, above all and by essence, a crime.

Trafficking in human beings is also something that has been present for centuries, in the form of slavery and serfdom, and later on with the modern exploitation of labour at the outset of the era of industrialization.

Even drug trafficking is not new. I don't need to remind you of the 19th century opium wars which took place not so far from where we are today.

That said, we can consider that there have been many significant changes in these fields in recent centuries and even decades. I will mention three that I find are incredibly noteworthy.

The first main change has been the major development in telephone and radio communication since the beginning of the 20th century into what we now call new technologies in information and communication (ICT). Prior to this development, it was extremely difficult, if not impossible, to communicate very quickly and from a long distance. Smoke signals, pigeons and semaphores helped, but with limited effect. These new technologies now make long range and immediate interconnections possible. If these

technologies have served, and are still serving, law enforcement agencies in a positive way, they can also be used negatively by criminals. The latter have been very quick to understand and take advantage of these new technologies to make their crime more profitable. In any case, what is really new is the speed by which information is propagated, with a huge evolution from the first phones to today's high speed and mega content internet. Today, a single laptop can be used for actions that have global consequences.

This innovation has led to what some now call the cyberization of the world. Although cyberspace is totally virtual (a computer virtual world), it is an extension of the physical space where the identification of criminals and preparing for any type of cybercrime or cyberattack is very difficult in terms of trying to document, identify and then attribute these crimes and attacks. The true revolution in this regard, I dare say, is that we have moved from visible crime to invisible crime. In this new era, it is far easier to instigate cybercrime than to counter it.

However, if the framework of the crime has dramatically changed, the paradigm remains.

The second alteration concerns borders. Before the 17th century, there were no real borders anywhere. When there were some, they were in fact either fluid or natural: rivers, mountains, the sea, etc. These elements changed in the wake of the Treaties of Westphalia (1648). Although the Treaties didn't firmly trace what were then the national borders of territories, the concept of the nation-state and sovereignty appeared and developed. These new borders gave state authorities the power to guarantee national sovereignty in a peaceful way and within a given space. Progressively, national authorities got more power in their respective territories. This evolution, moving through nationalism and post-nationalism,

turned into an issue as some countries were unsatisfied with their borders and tried to amend them to the detriment of others. This tendency reached its paroxysm with the Second World War. Thereafter and in reaction to that, Western Europe has tended to unite and to make borders as permeable as possible. In some other parts of the world, state borders are considered as rather artificial insofar as they divide ethnic groups. Today, as a result of terrorism and the migration crisis, we are back to more control of borders. So, borders are there, but their perception and reality are sometime evolving in time and space. In principle, individuals crossing borders require identity checks, passports or visas. Likewise, moving equipment and goods through borders is subject to taxes or customs fees.

Although the general trend of globalization is to ease border crossings, some borders have been made stronger for particular reasons. Even that reveals that borders are more and more leaky. If borders are easier and easier to cross for regular individuals, we can assess that they are roughly inoperable for criminals.

A third evolution is the exponential changes in demography with a mega-trend towards urbanization. At the beginning of the 19th century, only 3% of the world population was living in cities; today, this percentage is more than 55% and could go up to 65% by 2050². World-wide, twenty-eight mega cities gather more than 10 million inhabitants each. This brings a tremendous challenge to law enforcement agencies. Until the nineteenth century, police dealt with more territory and less with population. Now, the police have to concentrate their endeavour on cities. Any public event easily becomes a large-scale event where thousands of people meet. Commuters in conurbations number in the thousands every hour. The concentration of an important mass of people in a given and limited time/space frame constitutes a

security challenge because of cyber and/or physical threats. The life cycle of such events, from preliminary intelligence gathering to final planning, needs to be strengthened by experience and information sharing. An increased population with better conditions of life and improved mobility has led to mass tourism, which is another security concern for both transportation and tourist infrastructure. Populations are drastically increasing and moving from one state or one continent to another. However, these tendencies are not equally distributed world-wide.

So, if we consider these three evolutions together, what do we discern? More and more people communicating and moving on a larger scale and at a higher pace. From a police perspective, we therefore have fluidity and a volatility of risks and threats.

Transnational organized crime and terrorism can more easily flourish and proliferate on this new and troubled ground.

The challenge is now the competition between international criminal and terrorist rings and the police, as both use all of the up-to-date ways of communication and try to stay a step ahead on the most recent technologies. In this race, the police are quite often in the position to react, while criminals are quicker to identify potential uses of new technologies and/or any shortfalls in the judicial/law enforcement systems. Criminals are also quick to find a cheap way of doing their 'business', and the Police have to spend far too much money to fight this. At the same time, criminals and the police do not play in the same yard: there are no borders for new crime, but the Police still have to deal with them.

Therefore, international organizations dealing with law enforcement and police matters have to understand the actual issues and propose answers based on their respective mandates.

The OSCE is the World's largest regional arrangement under Chapter VIII of the United Nations Charter. It unites 57 participating States from Vancouver to Vladivostok and 11 Partners for Co-operation in the Mediterranean and Asian area. It gathers more than one billion inhabitants in the Northern Hemisphere.

Our intrinsic strengths are consensus-based decision making, inclusive membership and a multidimensional concept of comprehensive, co-operative and indivisible security.

The OSCE participating States believe unanimously that the politico-military, economic and environmental dimensions, along with the human dimension of security, are intertwined. Furthermore, one of our advantages includes a network of 15/16 Field Operations that provide specific, tailor-made and customer-oriented support to participating States.

Our comprehensive approach to security applies to any challenge.

In the field of transnational threats, the OSCE set up a specific department which deals with cyber, border, police and terrorism issues.

When it comes to dealing with any type of crime, there are three steps: before, during and after. My understanding of this is that the first and most important role of law enforcement is to deter and prevent a crime from happening. To stop it is already too late.

On this, I again refer to Sun Tzu when he said: "The greatest victory is that which doesn't require any battle".

In this field, the historical fight between the sword and the shield happens every day.

The OSCE is not an operational organization in a military or police sense; we work as a

platform to promote principles and values that all of our participating States have agreed on. Universal human rights, shared security and prosperity – the founding values of the OSCE and the United Nations – are for us the best antidote to organized crime, terrorism and violent extremism.

In addition to this message, which we convey to our participating States, we also provide technical assistance, expertise and support on request.

Transnational means, but not only, trans-borders. In that sense, one of the most important and concrete challenge to deal with is borders.

I will focus my last points on border-related issues, from an OSCE perspective.

Our endeavours aim at:

1. Enhancing inter-agency and cross-border co-operation; in 2016, the OSCE established multi-national and multi-agency mobile training teams for the identification and investigations of foreign terrorist fighters at borders (entry and exit border check points), in compliance with international human rights standards. The implementation of the project goes through the following phases. The first training is designed and delivered by international experts in order to identify suitable candidates for being member of a mobile training team. Thereafter, the identified candidates receive advanced training that helps to prepare them as future trainers within a mobile training team which is to travel to specified border crossing points to deliver tailored training. Then, the mobile training teams deliver specific training to personnel assigned to the designated locations. The training team comprises borders officers from various countries from the OSCE area. The training course delivered by these teams covered the effective use

of databases, detection of forged travel documents, risk analysis and management, understanding of behavioural indicators and included a table top workshop. INTERPOL is part of the project along with selected border and counter-terrorism experts from OSCE participating States and Partners for Co-operation. We are co-operating with other international organizations, such as UNODC, UNCCT, IOM and Frontex, and the teams are ready to travel around the OSCE area to train front-line officers.

2. Foreign Terrorist Fighters constitute one of the current threats to international and regional security. As terrorist groups come under increased pressure in neighbouring conflict zones, we are seeing an increase in the number of returning foreign terrorist fighters. Many of these individuals will try to use broken travel (eg flying to Africa/Asia and then taking flight to Europe) to enter the OSCE area or will use fake/forged identity documents to cross our borders. Therefore, identifying and preventing cross-border travel by FTFs is a way to address this threat, notably by using and promoting Travel Document Security/Advance Passenger Information (TDS/API) exchange system which allow States to check suspected terrorists against watch-lists before they travel. The OSCE is implementing capacity-building activities in this domain and encouraging increasing membership in the International Civil Aviation Organization's Public Key Directory (ICAO's PKD) (currently 29 pS and five PfC). The OSCE strongly believes that an increased membership in the ICAO PKD and broad awareness of the requirements to establish API systems are realistic goals enabling to better fight against FTFs issue. Our activities support the UNSCR 2178. More widely they aim at countering emerging forms of illicit cross-border trafficking, with a particular emphasis on irregular migration;

improving States' ability to detect both imposters and forged/fraudulent travel documents at the border-crossing points; and supporting participating States in improving the security of both e-passport and identity management systems (through development of compendium of good practices).

3. Delimitation and demarcation of borders remain an issue for many countries. The OSCE has supported a number of participating States in implementing its Border and Security Management Concept (adopted in 20015) with the aim to promote open and secure borders. Difficulties related to international border definition and the lack of demarcation and delimitation represent a challenge to territorial integrity and border security and management. From 2011, the OSCE has therefore organized seminars bringing together national experts from national boundary commissions in order to examine national experiences and technological tools related to border delimitation and demarcation. This remains a long process requiring deep and careful discussion and planning, addressing complex issues, notably legal. The OSCE provides a concrete platform to discuss them; to visit approaches, definitions, legal frameworks and national experiences; and to help participants familiarize with all facets of negotiations. During the latter, the challenge is to keep political points at bay and for the involved agencies to focus on technical issues. An OSCE Guidebook on Delimitation and Demarcation Practices is to be developed and published.

4. Promoting and supporting Police and Customs Co-operation Centres (PC3) in South-Eastern Europe. Operational cross-border co-operation needs to be enhanced and promoted at a local level. This could be done by establishing joint cross border

check-points in some critical locations where customs police officers from both countries can work together in the same facility. Once approved by national authorities, this goal could be reached by providing legal basis and developing common standards operating procedures. The OSCE has supported a number of initiatives in South-Eastern Europe in this regard, for example between Albania and the former Yugoslav Republic of Macedonia, and between Albania and Montenegro. In the same vein, the OSCE has assisted countries to achieve joint agreements as regards the so-called 'hot pursuit' process when police officers from one country can continue their investigation (flagrant crime) in the neighbouring country without lengthy procedure on borders. Some agreements were achieved on that between participating States in South-Eastern Europe.

I conclude my contribution on an optimistic note in line with what Mr Martin Wolf, a British writer in politics wrote recently, "The future does not have to be a disappointment".

¹The Art of War

²UN data



Dr Jean Salomon

Business Development Director
SICPA SA

Jean Salomon joined IBM France after his Ph.D, followed by 10 years in Medical Imaging overseas, first in R&D and next in the industry as European Product Manager. After a 20-year career with IER, in the design and marketing of secure Access Control and Passenger Automation equipment for the Transportation Industry, Jean worked for 8 years as Principal of JSCP, a consulting practice dedicated to Logistics, Travel and Security, with special emphasis on Border and ID management.

As an ISO expert, Jean is an active member of ICAO's NTWG and ICBWG, focusing on various ID- and IT-related components of Integrated Border Management Systems. He performed several TRIP assessment missions for ICAO, and is an advisor for E.U. FP7 projects. A frequent speaker and moderator at Industry forums worldwide, Jean has recently joined SICPA as Business Development Director in the field of Border Management.

SECURE BORDERS AND IDENTITY PRESERVATION IN THE DIGITAL AGE

*Authored by
Dr Jean Salomon*

Illegal and war-driven migration patterns, compounded with limited human resources to handle the growing amount of legitimate travellers, are putting a strain on current border clearance procedures in many parts of the world.

Automated border clearance procedures, biometrics technologies and a resilient cyber-secure IT infrastructure all need to meet in a coordinated way to provide an efficient shield against identity theft and its criminal consequences. At the same time, any form of digital transformation should also respect the regulatory frameworks of the citizens' privacy protection agencies in both origin and destination countries.

Goals and Challenges

In view of the seemingly conflicting interests of the major industry stakeholders, the focus of this paper is not to oppose "facilitation" to "security" during our discussion on border clearance and ID risk-assessment procedures. It is to establish which pillars sustainable ID security-driven processes can rely on to control the rapidly evolving threats that parallel the pervasive developments of the digital economy.

In current border crossing processes, both travel documents and biometric-triggered inspection systems will maintain their respective and complementary roles using physical document security during all required ID verification steps.

We shall thus review a few implications that tie physical and digital security features together, while looking at the evolving framework of establishing, maintaining and verifying one's identity.

Secure ID Management Scheme: Main Pillars

1. Relying on established MRTD standards: adapted priorities of the inspection systems

ICAO's Document 9303, in its last rewritten edition, has proven a great asset in formalising an up-to-date, itemised features list for compliance of all e-Passports. However, although ICAO has officially banned non-Machine Readable Passports as of the end of 2015¹, no requirement was yet issued to ICAO Member States to switch to e-Passports.

Also worth noting is that ICAO continues to actively promote the use of innovative physical security features in both MRTDs and e-Passports.

Even more noteworthy, in only 13 years, over 80% of regular world travellers are now in possession of an e-Passport. More pressure on destination border control authorities is expected in the coming 15 years based on IATA's world air traffic forecasts – mostly fuelled by Chinese tourists' e-Passports applications.

One of the main outcomes of the introduction of added digital security on e-Passports has been the decrease of usage of tampered documents, making room for a steep rise of impersonations (where an imposter -e.g. a look-alike- presents an otherwise genuine MRTD).

Conversely, and in spite of the rapid progress in installing Automated Border Clearance (ABC) e-Gates equipped with biometrics, ICAO Member States were slow in implementing standardised best practices of their respective IT border inspection systems.

The required breakthrough would involve timely exchanges of digital certificates between origin and destination countries which would in turn execute secure challenge-response protocols for e-Passport authenticity verification and confirm the identity match between the holder of the MRTD presented and its legitimate owner.

To speed up the adoption of these practices, ICAO has been heavily promoting a centralised Public Key Directory (PKD) certificate distribution centre. ICAO is actively pushing Member States to become members of its own PKD scheme (55 out of 191 Member States by end 2016), in order to provide a mechanism to centrally collect the certificates and redistribute them without the heavy burden of diplomatic bilateral digital key exchanges.

2. Large scale Entry-Exit systems and the overstayers issue: a need for a local, cost-efficient breakthrough

The disruptive effect of unexpected, war-triggered migration and the associated handling of refugees have strained both LEAs and specialized migration agencies' capacity to maintain a homogeneous level of border management practices across the various enrolment or verification crossing points in all modalities (e.g. air, sea, land).

Besides rapidly identifying criminals and other suspects, one of the major security issues is the identification of over-stayers, which include both visa-requiring and visa-exempt individuals.

As an example, Schengen Member States finally finalised their dual Schengen Information System – Visa Information System (SIS-VIS) IT infrastructure after many years of deferrals. Yet, current EU and national legislations still need further amendments to allow large-

scale database sharing across Member States (e.g. SIS, VIS and the asylum seeker fingerprint EURODAC DB). This is a prerequisite to requesting VIS biometric ID verifications of SIS queries. Additional legislative changes are still required to authorise the IT-driven biometrics EU Entry-Exit System implementation with a projected cutover in 2020.

Conversely, the United States – which currently has no manned exit border checkpoints – is actively revisiting this policy to match all departing non-American travellers' biometrics (at the gate of a boarding aircraft) with their own biometric tokens collected upon entering the USA.

Preventing ID substitution upon departure, and identifying overstayers are, therefore, achievable, pending the successful scalability up of such procedure across all border-crossing modalities (e.g. air, train, car, boats, and pedestrian crossings). But are such procedures scalable – budget-wise – across all border points and border-crossing modalities (e.g. air, train, car, boats, and pedestrian crossing)?

3. Evidence of identity: from weak link to opportunity

Because of e-Passports' combination of enhanced electronic and physical security features, ID document fraudsters rapidly turned to the more fragile part of the document ID security value chain by counterfeiting or altering "breeder documents" such as births or deaths certificates.

Since these paper documents bear little or no protection and lack proper worldwide standardisation, the insertion of forged identities into an otherwise genuinely authentic travel document (including e-Passports) started to gain traction.

ICAO has recognized the importance of

securing breeder documents and set it up into its world TRIP programme with a high priority. However, practically turning around the intrinsic breeder document weaknesses will require time for each country involved, especially if sought in a harmonised way.

Border ID Security Success Implies Stakeholders' Consensus: Air Transportation Case

1. Nowadays, air travel processing begins at home, through an efficient "space-warping" check-in implementation

It is worth noting that both air carriers and airport integrators have bolstered productivity from the late 90's on, by expanding the airport premises beyond its physical boundaries; that is "warping" the space domain to expand the airport's logical boundaries to the traveller's home.

Early internet check-in and smartphone boarding passes led to streamlined check-in procedures, with a controlled access to the airport's "sterile" area to undergo further bags, ID and border checks. The reason for success lies in an early industry stakeholder consensus (i.e. carriers, airport systems integrators and Control Authorities) that jointly developed worldwide electronic ticketing standards and common airport passenger flow procedures.

2. Similarly, border crossing starts at home as well, under an elaborated "time-warping" scenario

The same reasoning of "warping" the time domain can be applied to the advantage of the receiving country. Voluntary data transmission of border security-related information could be initiated as soon as an international travel plan starts to mature, even before the final booking, thus providing ample time to perform advanced clearance investigations prior to the traveller's arrival.

Many countries have considered implementing both Advanced Passenger Information (API) and Passenger Name Record (PNR) programmes, through which the traveller's identity (i.e. his passport's biographic data page) and all associated reservation data (payment and travel details) are transmitted ahead of time to the receiving country for proper risk-assessment. In air transportation, API data is collected and stored by the carriers or the airport authority, while PNR data is gathered by the Computer Reservation Systems (CRSs) at the time of the ticket purchase.

While many countries have already implemented API programmes, PNR programme developments are less advanced and more complex in nature.

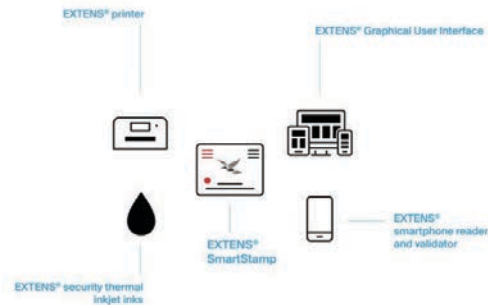
PNR programmes preventively activate systematic data mining on reservation details, acting as a can opener to seemingly limitless external queries (e.g. including credit card usage and social networks). Domestic privacy assessment regulations and the overall implementation cost and complexity are an important part of some of the observed PNR project implementation delays.

3. Is there a way to address the overstayer challenge at lower cost with more tangible and immediate results?

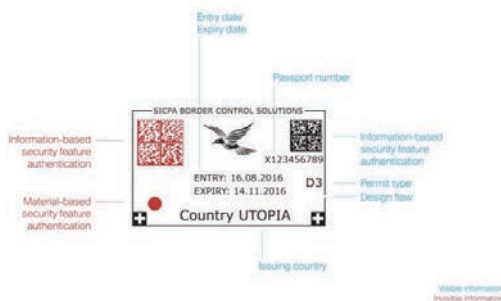
Deploying Dynamic Travel Information on MRTDs: EXTENS® SmartStamp and Overstayers Detection

The travel document presented to support the visitor's credentials remains a core part of the ID verification process during a border clearance. There is an opportunity for a destination country to significantly improve the registration and retrieval process of successive entries and exits, while enhancing ID verifications using the document itself in a stand-alone

mode, independent of any pre-existing or upcoming online IT border management infrastructure.



The idea behind it is to replace manual stamping with an automated stamp (or visa) printing at the point of entry, in a secure form (i.e. using a digitally sealed 2D bar code) containing a log of the event's key descriptors such as the crossing location, time of stamping, agent ID, specific passport details and visit category, and so forth.



Automated read-back of this information would immediately reveal an overstayer status, either during a roving surprise ID verification by LEAs, or at the occasion of the planned exit at the border checkpoint. Advanced stamp protection could also include dynamically applied material science-based security features (e.g. binding the stamp printer ink with the document itself).

Such digital stamping processes would also eradicate fraudulent activities such as old stamp alterations, theft, loss and misuse of

manually applied rubber stamps applicators. Since the background image of the digital stamp could be downloaded at will from a central distribution point reaching out to all entry border checkpoints, forged stamps or visas sometimes created to “decorate” new passport fakes could be easily revealed, even by simple visual inspection.

It is worth noting that such a dynamic stamping process is not limited to MRTDs during border clearance. It could also secure other types of breeder documents presently deprived of any protecting scheme (e.g. birth certificates). It could also be implemented as low-cost, standalone tools in cooperative regional border agreements using commonly agreed transit tokens for roving controls in remote areas, away from any central border management systems.

Conclusion

As far as practical implementation is concerned, identity document security must be preserved in order to empower the rights of owning, protecting, and using one's legitimate identity.

Robust physical security features embedded into the paper of the travel document remains a critical protection scheme of the MRTD in the hands of its bearer. Linking both physical and logical/digital security tokens has already proven beneficial, if correctly and uniformly deployed in the e-Passports delivered to the citizens.

Today, MRTD application and retrieval of dynamically variable, yet secure registration tokens such as SICPA's EXTENS® SmartStamp will promote low-cost registration and tracing of the growing traffic of legitimate Third Country Nationals (TCNs) travellers across many borders with minimal (or no) IT infrastructure requirement. The same processes and tools can be used to enrol and trace unexpected migratory flows using any specific physical document service platform for both enrolments and verification.

In the future, the overwhelming increase of connected digital objects and processes may integrate embarked sensors and mobile platforms to perform on-the-move, sustainable, decentralized ID assessments. Thus, maintaining a continuous credentialing system linked to one's identity may become a moot point in a more distant future.

What may become less significant, thus, may be the information highways themselves, where patrolling cyber security agents will have a drastically evolving role to play. In a new paradigm of worldwide logistics beyond the level of Amazon's current Web Services, information, goods and real travellers will have switched to an assumed (encrypted) identity while travelling the highways in an anonymised fashion.

Controlled entry and exits roads from these informational channels will be the only place for authorizing ID discontinuities through proper credentialing under an I-a-a-S (Identity-as-a-Service) scheme. Citizens' requests will activate swapping between commodity-driven identities usable in and out of a given highway, according to his needs, yet under unwavering credentialing control.

Emerging digital ID security tokens would retain material-based components with evolving form factors to lock each token with its legitimate owner, as key enabler to enter or exit trusted, anonymised Agora of information and services.



Dr Enrique Segura
President & CEO
Securiport LLC

Dr Enrique Segura has held executive positions within the financial and service sectors for more than 30 years and has extensive experience working with governments and managing large international companies. He is currently Chairman of the Board of the ENSE Group, a holding company that retains majority interest in the following companies: Securiport LLC, Alex Stewart International LLC, KIBO Laboratories, and Harbass LLC whose network extends to more than 64 countries worldwide, with a staff of 15,000 and an annual turnover of US\$1.8 billion. Dr Segura leads Securiport LLC as President and CEO. Securiport LLC provides civil aviation and immigration security services to governments based on the comparison and analysis of biometric data and traveler information collected during immigration processing.

Dr Segura is a member of the Board of Directors of the Trust for the Americas of the Organization of American States (OAS), where he also served as President from 2000-2004. Since 1996, he has been the Honorary Consul of the Republic of Uganda in Argentina. Dr Segura is also a member of the Board of Trustees of The Catholic University of America. He holds a PhD in Economics and is a graduate of the Harvard Business School.

STOPPING THREATS AT THE BORDER WITH THIRD LINE THREAT DETECTION

*Authored by
Dr Enrique Segura*

Threats at the Border

In the 21st century, Persons of Interest (POIs) – terrorists, narcotics smugglers, human traffickers, and other criminals—are constantly on the move, changing identities as needed to travel undetected. Widespread identity fraud combined with the ease of acquiring travel documents on the Dark Web challenges demographic-based matching techniques and puts travelers at an increased risk of identity

theft. Detecting persons of interest and other threats at the ports of entry and departure requires application of current-generation technologies and practices, but must go beyond these techniques to keep pace with the threat landscape. We can organize these detection and defense mechanisms into three lines, each of which provides critical decision support information at different scales to give us defense in depth at the border.



OFFICER DRIVEN THREAT DETECTION

- Automatic Travel Document Validation
- Watchlist Matching
- Observational and Behavioral Analysis



EXPERT DRIVEN THREAT DETECTION

- Threat scoring rules created by expert analysts
- Integrated Non-Immigration Data Sources



ACTIVITY BASED THREAT DETECTION

- Multi-dimensional traveler segmentation
- Pattern Detection
- Dynamic threat scoring

The Immigration Officer is the First Line of Defense

The first line of defense is the immigration officer, who analyzes the traveler's behavior while using the capabilities of the immigration control system to validate the traveler's documents and check against watchlists such as INTERPOL's I-24/7 system. This first line of defense is constrained by the officer's training, the capabilities of the immigration control system, and the number of passengers to be processed. This line is hard to scale beyond



these limits because humans are error-prone – for example, the United States of America’s Transportation Security Agency (TSA) agents failed to detect smuggled contraband 95% of the time when officially tested in 2015¹. However, officers hold the authority to make judgments based on policy and law, and have unique spatial analysis, reasoning, and cognitive capabilities that make them superior to machines at anomaly resolution. The other lines of defense, therefore, must provide the officer with anomalies to resolve, allowing them to move from monitoring travelers to addressing potential threats.

Expert Knowledge Forms the Second Line of Defense



The second line of defense uses expert-driven threat detection to discover anomalies for the immigration officer. Since an expert cannot be present to analyze every traveler, this line involves automating the expert’s knowledge. A common approach is to have experts create rules to “score” each traveler against known threat profiles. The rules engine alerts immigration officer to anomalous scores, and acts as decision support as the officer makes a clearance decision. Since each nation faces different threats, each requires different criteria for scoring potential threats. Likewise, each nation must be able to apply its sovereign data sources to this challenge. For example, a nation can integrate a national tax database

with the immigration data, so that an expert can compare traveler income records with flight and accommodation data to generate scores related to money laundering. This second line of defense is powerful and scalable, but is limited by the experts’ ability to generate and update rules based on the ever-changing threat landscape.

Dynamic Threat Analysis and Detection is the Third Line of Defense



The real-world threat landscape requires advanced and dynamic threat detection – the third line of defense. The third line of defense divides travelers into groups for analysis, monitors activities across the threat landscape, looks for patterns across travelers and threats, and adjusts its detection strategies to match changes to the risk landscape. Officers are continuously alerted to anomalies within their area of authority. This presents the immigration officer with both predictive and reactive information on which to base their decisions. In the background, experts orchestrate and guide the entire process, but the machines adapt the rules independently, reducing the scalability issues faced by the second line.

The Third Line of Defense



Threat Landscape Modeling – What and Where are the Threats?

The Threat Landscape answers the questions “what are the threats?” and “where are they coming from?” We cannot address traveler threats without understanding the overall threat landscape. The threat landscape is complex and ever-changing, and we must be able to represent it in a way that humans can understand and machines can process. We call this the threat landscape model.

Models can range from simple (the original color-coded US Homeland Security Advisory System) to complex (loss models that drive the terrorism insurance industry). The more complex the model, the more resources are necessary to groom and maintain. For traveler threat modeling, we must have a balanced and sustainable model that creates an illuminating and useful representation of the threats we face.

The threat landscape for travelers is composed of geographic, organizational, economic, social, political, physical, medical, and even cyber elements. By modeling and analyzing these elements and associated trends, we create

indicators of what type of threats are in play, the likelihood of those threats occurring, where the threats may arise, and what the targets of those threats may be.

Multi-Dimensional Traveler Segmentation – Who is the Traveler?

Market segmentation has been used for years in advertising, and are actively used today to match people with goods and services they have searched on the web. By applying segmentation strategies to travelers, we bolster the third line of defense by grouping travelers to make them easier to analyze. Experts can write segmentation rules. To provide truly dynamic traveler segmentation, we can use machine learning techniques to discover segments and threats that human experts could not easily generate. These techniques have proven highly accurate in situations such as classifying terrorist eventsⁱⁱ and can be applied to locating potential threats among travelers.

Grouping travelers into segments, scoring how strongly they “belong” to segments, and dynamically updating both as new data is available provides valuable information to

investigators about a traveler, while supporting officer decision making at the first line.

Activity-Based Intelligence (ABI) – What Happened?







ABI is an analysis methodology which rapidly integrates data from multiple sources centered

around the interactions of people, events, and activities in order to discover relevant patterns, determine and identify change, and characterize those patterns to create decision advantageⁱⁱⁱ. We must analyze travelers, travel-related national and global events, and traveler activities in association with threats represented by elements of the threat landscape. This requires processing of data from immigration and border control systems, data from governmental databases, and data from open and unstructured sources. From this data, we extract entities and events and link them together for investigation.

ABI requires a marriage of expert border security and threat domain knowledge, intelligence analysis, and data science – and these skills are challenging to find. We must, therefore, provide our investigators and existing analysts with robust and integrated information technology solutions to enable them to perform ABI at the speed of international travel.

Securiport Solutions

 <p>IICS Integrated Immigration Control System</p> <p><i>Interactive collection and processing of travelers at airports and frontiers</i></p> <ul style="list-style-type: none"> • Travel document scanning and validation • Biometric enrollment • Watchlist, fraud, traveler risk, and Interpol checking • Customizable reporting and dashboards • Support for multiple scanning and ABIS solutions 	 <p>eGate Automated Electronic Gates</p> <p><i>Automated enrollment and verification for an enhanced traveler experience</i></p> <ul style="list-style-type: none"> • Fully automated electronic gates • Automatic eligibility checking and determination • Integrated with IICS for watchlist, fraud, and Interpol checking and with IIMS for traveler risk assessment 	 <p>eVisa Visa Management System</p> <p><i>Complete management of the visa creation and validation process</i></p> <ul style="list-style-type: none"> • Manages all aspects of visa issuance, management, and expiration • Deployable across multiple locations (embassies, consulates) • Integrated with IICS for watchlist, fraud, and Interpol checking • ICAO compliant system 	 <p>IIMS Intelligent Information Management System</p> <p><i>Risk analytics that assess travelers against government and open data sources</i></p> <ul style="list-style-type: none"> • Customizable Person of Interest profiles generate real-time risk scores for travelers • Data integration for open source & national databases including unstructured data • Interactive data exploration and investigation for forensic analysis
--	--	--	---

Securiport's Layered Defense Solution

Our Integrated Immigration Control System (IICS) provides tools for the first line of defense – decision support for the immigration officer driven by travel document validation, identity fraud detection, checking against INTERPOL and local watchlists, and multi-modal traveler biometric analysis. Immigration officers and supervisors are presented with a cohesive picture of all travelers moving across the border, whether through manned posts or through our eGate Automated Border Control gates. We maximize traveler experience while providing the officers with warnings when a possible threat is detected. IICS supports remediation of the issue, to include presenting information useful in secondary screening or for quickly identifying and remediating false positives.

Our current-generation Intelligent Information Management System (IIMS) provides the second line of defense – expert-driven threat detection. Our Data Source Manager allows integration of immigration, governmental, open source, and unstructured data into a virtual data sets that create a basis for analysis. Our Profile Manager enables experts to create rules-driven profiles against these virtual data sets to analyze and identify Persons of Interest (POIs). These rules then inform users of the IICS system when POIs are traveling and provide additional decision support information to the officers monitoring the immigration or border control system. A small number of experts can, therefore, support a large number of immigration officers.

Using our eVisa system, Securiport clients can engage the first and second lines of defense before a traveler arrives at the border. All Visa applications through our system provide the full battery of biometric, watchlist, fraud, and POI profile checking using the information from the web-based Visa application in combination with biometrics and other information gathered during traveler interviews at embassies or

consulates. Pushing these lines of defense out is a game-changer for prevention.

Securiport's current-generation third-line of defense capabilities are our Learning Agents and our Discovery and Investigation solution. Learning Agents perform statistical or deterministic analysis over data sources exposed through Data Source Manager, and in turn provide their results as data that can be incorporated into POI profiles. Discovery and Investigation provides a graph/link based visualization and exploration tool for data in the system, allowing analysts to forge connections between travelers and identify patterns that may indicate threats.

The future holds third-line capabilities in the form of our Next Generation IIMS, a revolutionary expansion of machine-driven threat detection in the border security arena. Securiport researchers and engineers are developing big data solutions for advanced and near-real-time threat modeling, detection, assessment, and remediation that includes a full suite of analysis, visualization, and case management tools for end users.

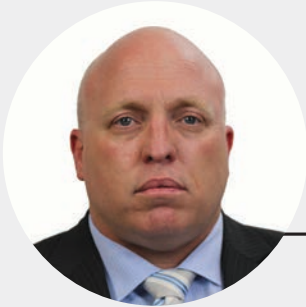
Detecting and Stopping Threats at the Border

Securiport's integrated solution provides threat detection and decision support tools for officials working across the border protection domain. From the immigration officer to the threat expert to the intelligence analyst, Securiport's tools enable layered defense across the first line, the second line, and the third line. This is The Science of Safer Nations™.

ⁱ <http://www.cnn.com/2015/06/01/politics/tsa-failed-undercover-airport-screening-tests/>

ⁱⁱ Khorshid, Motaz; Abou-El-Enien, Tarek; Soliman, Ghada; "Hybrid Classification Algorithms for Terrorism Prediction in Middle East and North Africa", International Journal of Emerging Trends & Technology in Computer Science, Volume 4, Issue 3, May-June 2015

ⁱⁱⁱ Atwood, Chandler "Activity Based Intelligence: Revolutionizing Military Intelligence Analysis", Joint Force Quarterly 77, April 2015



Dr John William Coyne

Head of Border Security Program
Australian Strategic Policy Institute

Dr John Coyne joined ASPI as the Senior Analyst for the Border Security Program in February 2015. John is currently the Head of Border Security Program of ASPI. John comes to ASPI from the Australian Federal Police, where he worked on transnational serious organized crime, national security, and counter-terrorism. Over the last twenty years he has been an intelligence professional at tactical, operational, and strategic levels across a range of military, regulatory, national security and law enforcement organizations. During this period he has worked extensively in the ASEAN region, delivering a range of bilateral research projects. His more recent work in this area has focused on enhancing multilateral ASEAN information exchange regarding non-traditional illicit commodity flows. John's PhD examined strategic intelligence in law enforcement targeting transnational serious and organized crime. He has written and published on a range of border security and intelligence issues. He has been a Winston Churchill Fellow and a Vincent Fairfax Fellow. John's border security research interests include intelligence, private/ public sector cooperation in the border environment and integration of border security operations.

VISION, INNOVATION AND COOPERATION: AUSTRALIA'S BORDER OF THE FUTURE

*Authored by
Dr John William Coyne*

Introduction

During the 1990's there was a glimmer of hope that the fall of the Berlin Wall and the rise of globalization might have marked a tipping point towards a '*borderless world*'. Futurists at the time were ambitiously interpreting global supply chain development as another step towards a world where people could freely move across international borders. But the September 11, 2001 terror attacks on the United States of America (US), assured the return of the securitized and militarized border paradigm. In the 16 years that have passed, border security has become a central and highly volatile public policy issue across the world.

The challenge for law enforcement officers and policy makers alike, is that the border security operating environment and threat context – especially within the air travel sector – has dramatically changed in terms of volume and speed. The traditional border security models of physically checking each arrival are no longer practical. Arguably, the policy responses to this challenge need to be underpinned by a paradigm shift.

This chapter will provide an explorative case study analysis of a recent border security innovation experiment in the international air travel channel by the Australian government. The chapter explores how Australia's efforts to innovate border security at Canberra International Airport represents a significant paradigm shift in the way it conceptualizes risk based border security decision making, technology development and private public sector cooperation.

Threat and risk at the Border

The breadth and complexity of threats make today's borders particularly tough to secure. Unfortunately, the current discussions on border

security are ever more polarized into a '*secure*' or '*insecure*' ultimatum. But for border agencies, there is far more to border security than law enforcement. The efficient and effective management of national borders is predicated on achieving harmony between security functions and border facilitation.

Unsurprisingly then, prevailing policy thinking constructs the border as a geographical point that must be controlled or secured physically. In this construct anything that crosses the border is assessed to identify whether it's likely to cause danger, harm or loss. When it comes to commodities, these kinds of assessments are relatively easy. Cocaine is illegal in Australia, and it has been assessed as a threat to the community. If cocaine is detected at the border, it will be seized. In contrast, the assessment of the threat and risk posed by individuals crossing the border is much more problematic. When it comes to the assessment of risk and threat posed by an individual, borders are arguably not just a physical point of control. Rather, they are a transition point for changes in the nature and scope of risk or threat posed by that individual.

It's clear that many national and domestic security risks have a transnational dimension that's transformed through the border. In this construct, the national and domestic security challenges at borders don't just relate to border transaction per se, but to the assessment of the likelihood that national and domestic security risks will be realised.

Australia's Response

The first phase of Australia's policy response to the changing border security environment involved substantial structural and policy changes. In May 2014, the Australian government announced significant changes to the way its borders were to be managed.¹ On the

1st of July 2015, the Department of Immigration and Border Protection (DIBP) and the Australian Customs and Border Protection Service officially amalgamated into one department. At the same time, a new frontline operational enforcement arm – the Australian Border Force (ABF) – was established. The ABF consolidated operational staff from both agencies into a single organisational and command structure.

The second phase of Australia's new strategy has been to create depth within their border security measures. Through a continuum model Australia has elongated its border to allow for security decisions – including those concerned with the disruption of potential threats and risks – well before the physical border.

Despite this change, the scale of border security transactions in Australia still puts immense pressure on ABF and DIBP facilitation and intervention capabilities.ⁱⁱ In response, Australia is driving another paradigm change in which its strategy is shifting focus from managing transactions to disrupting and mitigating border security risks. This change will be particularly important in managing risks in the air stream. In a simple sense, the number of deviant travelers in the Australian air stream is statistically small. Through careful intelligence based risk assessments it is possible to identify the low risk travelers. And with this assessment, it is then possible that the majority of low risk travelers could be safely granted entrance to Australia with limited or no physical interaction with border agencies. In this context, the DIBP's and ABF's continued development of intelligence-led and risk-basedⁱⁱⁱ enforcement strategies isn't a catchphrase, but an organisational imperative.

The Vision

Australia's border security strategists have developed a clear vision for the air travelers' experience at the border. In this vision, the majority of travelers (perhaps as high as 90 to 95 percent) will exit their planes on arrival and

walk to the arrivals hall to collect their baggage with no physical contact with border officials. Australia is not alone in this thinking: new technologies for biometric facial recognition and risk management are being trialed in airports from Singapore to Dallas Fort Worth. But, the strategy being considered in Australia is as much about new policy and strategy as the acquisition of new technologies.

Building the future airport border

In December 2016, Australia set in train an audacious paradigm shift in border security with a simple request for tender (RFT).^{iv} Rather than articulating the specific technical innovation required, the RFT provides a framework for establishing a collaborative innovation relationship focused on an outcome (the vision) not just an output or deliverable (specific technology). The complexity of this project is illustrated by the way various media outlets misunderstanding the scope of the project to mean an end to passports by 2020.^v

The project RFT sought a 'service provider' to develop an automated processing solution to support the concept of 'seamless traveler' movement through the Australian border protection process. The service provider will:

1. Replace Australia's existing physical passenger arrival card with a solution that collects the same data and automatically migrates this data to DIBP's existing systems.
2. Develop, supply and implement a solution at the existing points of automated border control and primary line that will *'eliminate the need for physical tickets and have the ability to process travelers using 'contactless' technology, removing the need for some travelers to present their passport.'*^{vi}
3. Develop and implement a system that will replace existing exit marshal points or secondary line processing. The solution needs to remove the need for a manual triage process at these points.

The service provider for the RFT is expected to provide infrastructure (hardware and software), installation and proof of proposed solution in a lab environment, pilot at the nominated airport (Canberra^{vii}) and rollout to nine (nine) other international airports.

In time, this project may revolutionise border security arrivals processes in terms of traveler experience and enforcement operations. While predicting the exact types of technologies and processes likely to be developed is difficult, it is reasonable to expect the following:

- Travelers will likely be asked to electronically complete an e-arrivals card replacement on check-in, using a range of access devices.
- It is possible that traveler biometric data will be captured on check-in at the departure point.
- During transit, DIBP and ABF systems will undertake a real time enhanced risk assessment of each traveler with the aim to identify the high risk travelers. The early completion of the e-arrivals card replacement, and biometric data, will provide additional information for the conduct of what will largely be an automated risk assessment process.
- On arrival at the destination airport, a combination of facial recognition biometrics (captured on the move), and data matching is likely to be used to identify travelers. This process will likely pose the most challenges. Emerging camera technologies and facial recognition software exist, but integrating these in a system with the desired level of accuracy will be challenging.

For the majority of travelers, possibly 80 to 95 per cent, there will be no physical interaction with border officials or border processes. For the ABF the only process that will likely remain manual will be calling out and checking passengers

deemed high risk or anomalous passengers.

The project's success will likely be dependent on at least three factors:

- The identity management system, and its associated biometric collection points, need to be able to maintain a high degree of accuracy.
- The new system will need to be able to uniquely identify travelers from the moment that they present at the departure check in lounge to the point that they leave the arrival terminal.
- Each traveler's identity, and its unique biometric identifiers, need to be stored so that they can be matched against travelers in the future.

Should Australia want to champion a universal biometric identity travel system, without the need for passports at all, it will require 'buy-in' from a critical mass of countries who are willing to collect and share biometric data. Such a universal system is well outside of scope for this Australian project given the immense cost, privacy and security implications. Understandably, these factors also make a universal biometric identity travel system appear unlikely for the foreseeable future.

In contrast the Australian system will likely be dependent on airlines at the point of embarkation. Most likely, airlines will be asked firstly to confirm the authenticity of travel documents. Already airlines like Emirates operate world class document examination processes so this is unlikely to be a significant barrier. Secondly, airlines will then need to compare the travelers biometrics to those contained in the travel document (most likely photographs) to confirm identity. The introduction of a standardized identity confirmation at check-in is unlikely to be a significant barrier to implementation of this project: for the most part there are already similar manual processes already in

place. Finally there would be a stage where the passenger information, including biometrics, are sent to Australia in advance of the passenger arrival. While advanced passenger information, including passenger name records (PNR), are already transferred to Australia authorities for all arriving aircraft, the provision of additional biometric data will have bandwidth, privacy and security implications for the Australian authorities.

The risk management system that sits behind this airport solution will be another factor for success. The algorithms that will be the lifeblood of this system, will need to be continually reviewed to account for the agile nature of threats posed by transnational organised crime (OC) and terrorism. While historical patterns of criminality will provide indicators and then warning of increased risk, border agencies will need to remain wary of sudden changes in criminal methods. The ABF's existing human observation and behavioral profiling methodologies will remain critical for early warning and agile responses to threat environment changes.

This project radically departs from current border security norms in that it will clear some passengers without the need to show or scan passports. While existing smart/E-gate systems are fully automated, they still require the scanning of passports. The new arrangements will drastically improve the traveler experience for the majority of those arriving into Australia by reducing processing times. At the same time, the ABF's finite operational resources will be channeled towards the travelers who represent the greatest risk.

Border security measures being increasingly pushed to the back rooms of airports beckons questions regarding impacts on the deterrent effect of visibly border entry officers and public confidence in agencies. Put simply, it looks like the borders of the future will not appear securitized, despite the use of more

accurate systems. The question for border agencies is whether the absence of a visual security performance will contribute to an increase in border deviance.

Conclusion

For the time being, any hopes that international borders will become redundant has passed. The world has entered a period where borders are more important than ever. Borders have become another important layer in a countries defence against threats such as transnational OC and terrorism. The key to meeting the current border security challenges is innovation. But innovation is not just concerned with the introduction of new technologies. Instead, it deals with dramatic paradigm shifts in the way border agencies think. Only time will tell whether the Australian approach will deliver the results it promises. And for the public success may in fact look like less rather than improved security.

¹⁵S Morrison, 'A new force protecting Australia's borders: address to the Lowy Institute for International Policy, Sydney', media release, 9 May 2014, online

¹⁶DIBP, 'Australian Customs and Border Protection Service: Agency resources and planned performance', 2014–15 Portfolio Budget Statements, p. 89.

¹⁷The term intelligence-led describes a business model and managerial philosophy in which data collection, collation and analysis (from a threat perspective) contribute to objective decision-making on problem reduction, disruption and prevention through strategic interventions. In risk-based systems, information about the likelihood and consequences of one or more unwanted outcomes is collated and analysed to assist decision-makers.

¹⁸<https://www.tenders.gov.au/?event=public.atm.show&ATMUUID=35574EFC-0FA4-C2D6-8B2628BDECC89867>

¹⁹<http://www.stuff.co.nz/travel/news/88700690/End-of-passports-Australias-government-moves-to-radically-overhaul-international-airports>

²⁰<https://www.tenders.gov.au/?event=public.atm.showClosed&ATMUUID=CB5B8563-D938-17BF-FEFAE9E007CF0AAF>

²¹The Canberra Airport is the airport serving Australia's capital city, Canberra. The airport was a domestic terminal until January 2016 when Singapore Airlines announced four weekly flights from Singapore to Wellington via Canberra with a Boeing 777-200 aircraft. It presents as an excellent test location for border security technology because of its small size and limited flights.

www.interpol.int

