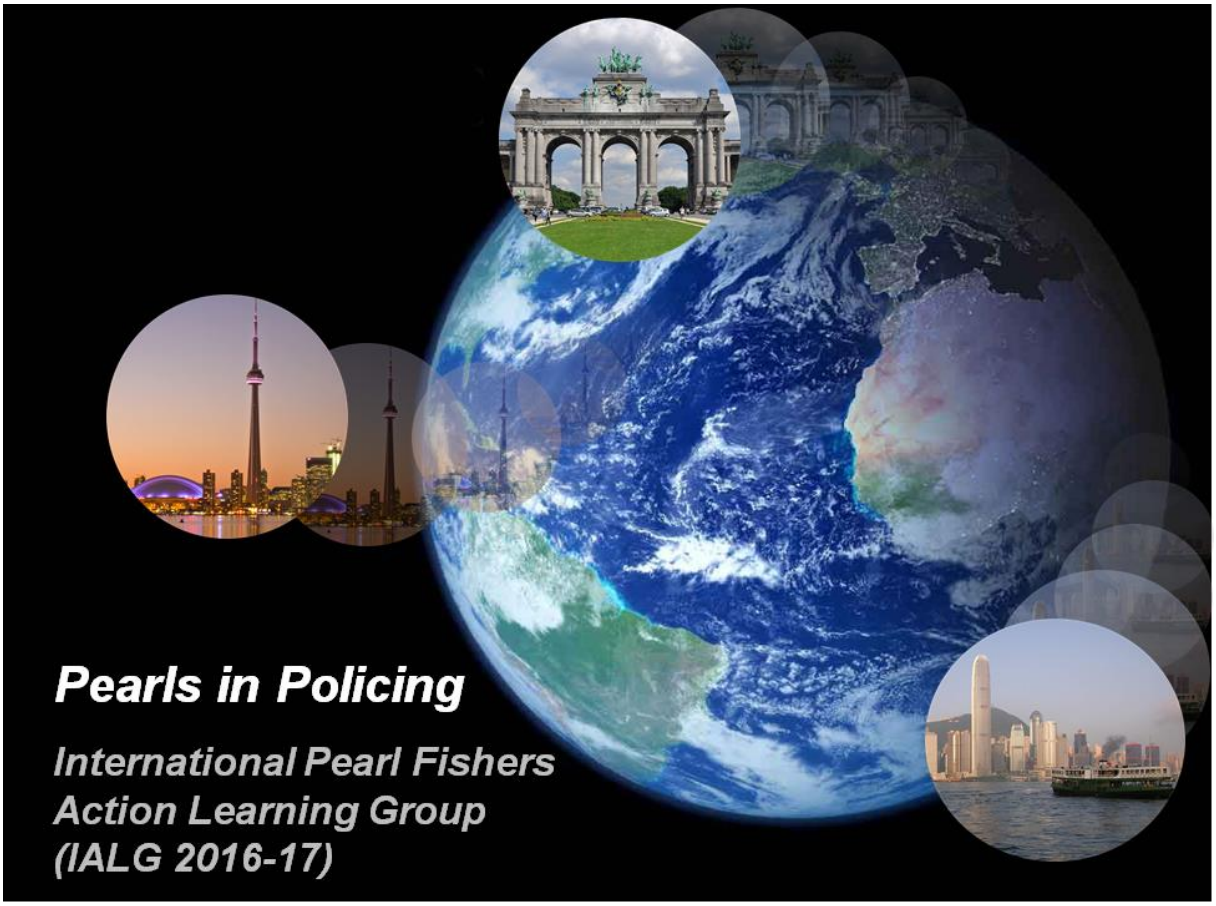
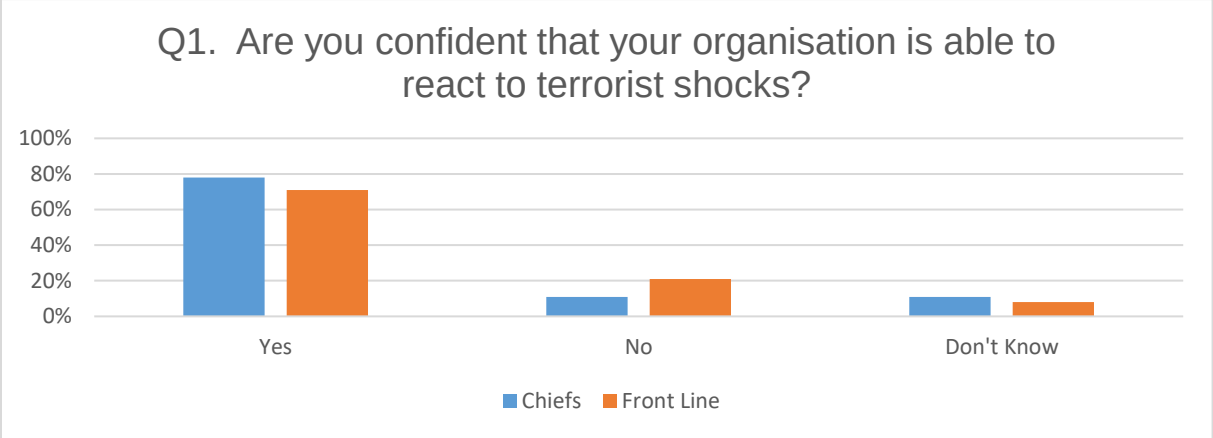
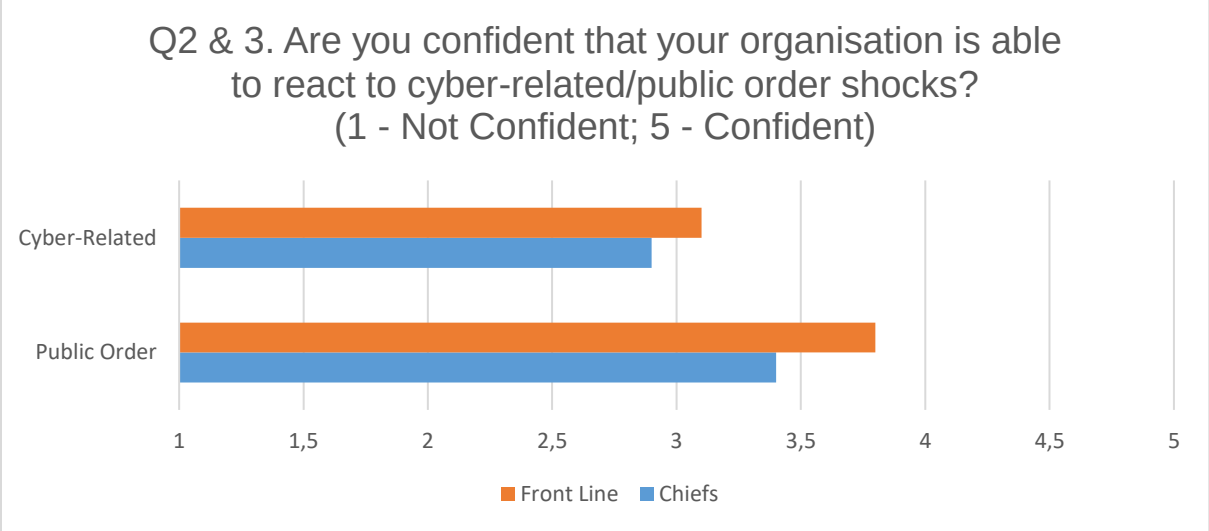

Pearls in Policing
International Pearl Fishers
Action Learning Group
(IALG 2016-17)

1 Table of Contents

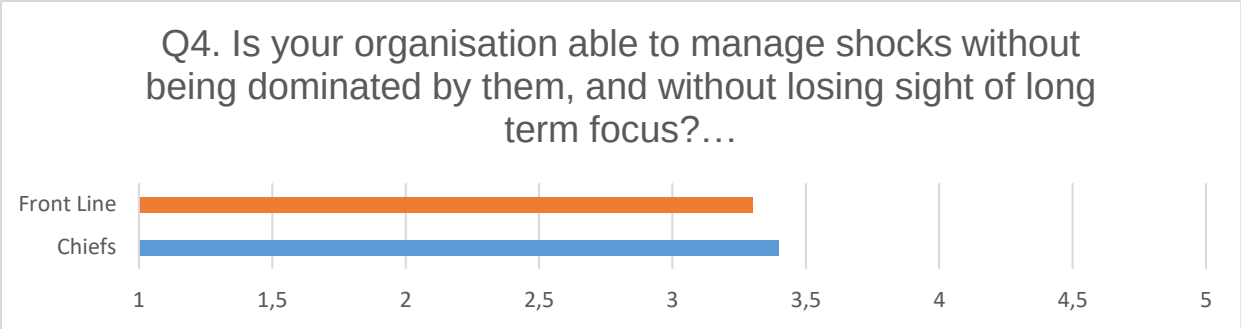
2 Polling results from the chiefs of police and front line members





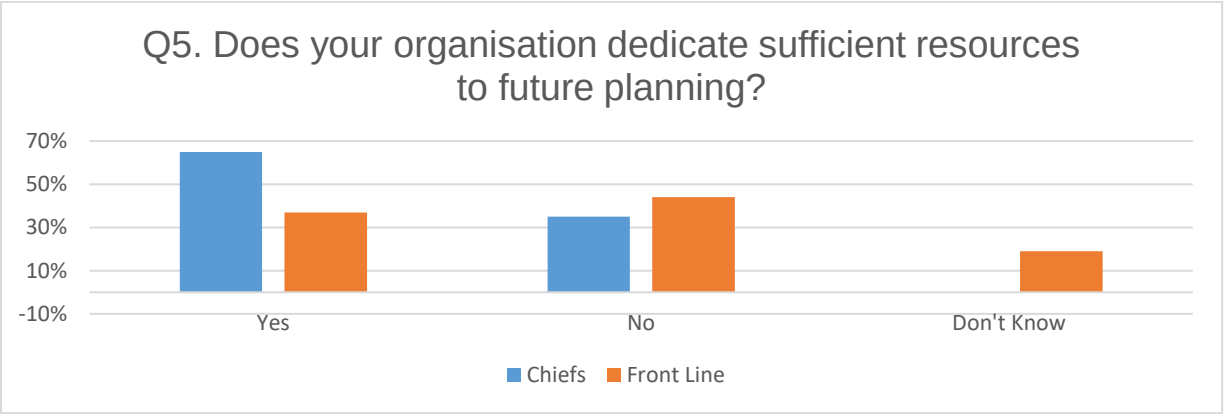
Commentary on Q1, 2 and 3

A high level of confirmation by both the Chief Commissioners and Front Line members that their organisation is capable of reacting to terrorist incidents and public order shocks, but capability to react to a cyber related shock is seen as the greatest vulnerability of the three.



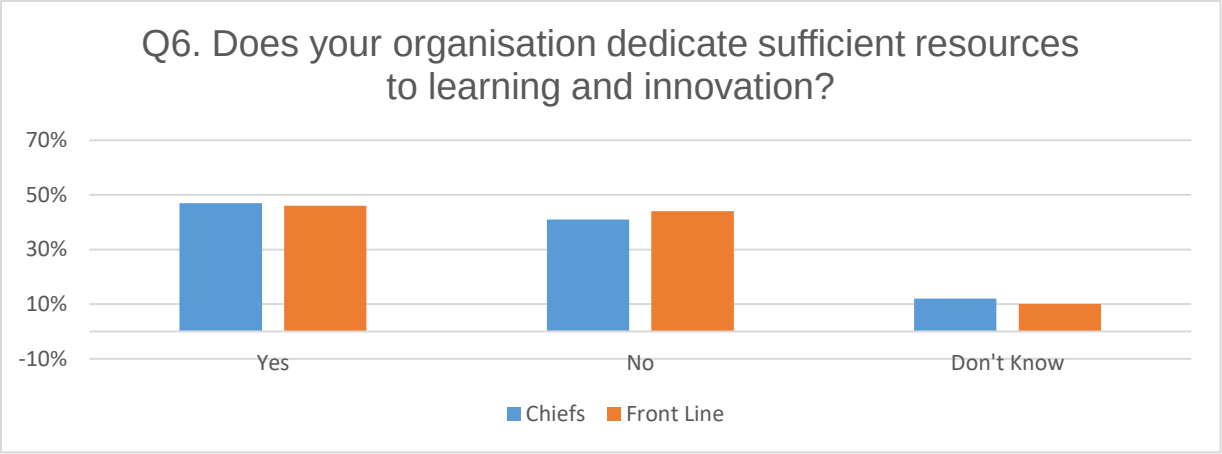
Commentary on Q4

The ability for the organisation to return to key priorities/core business without being dominated or distracted by shocks sat at 3.3 – 3.4 (on a scale of 1 to 5, with 1 being not able to return and 5 being able to return). This indicates there is room for improvement and perhaps a need to identify what factors may be impacting on the organisation's flexibility and resilience.



Commentary on Q5:

The commitment of resources to future planning was more positively reflected by the Chief Commissioners as compared with Front Line members who showed a higher response in the negative and unknown categories. This could be a reflection that members are unsure of the organisations' long term plans and future strategic direction. Even amongst the Chief Commissioners, only 2 out of 3 agree that sufficient resources were dedicated to future planning indicating further room for improvement.

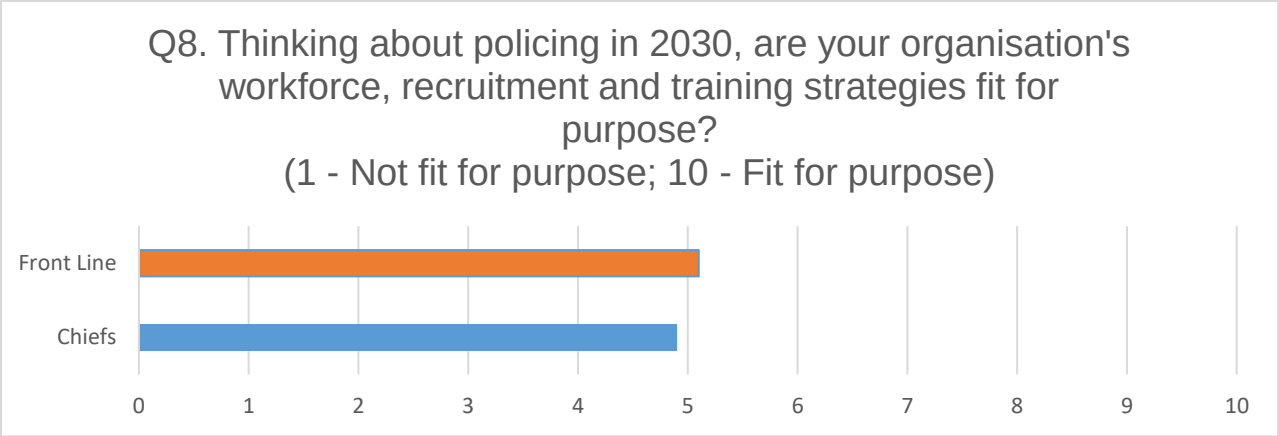


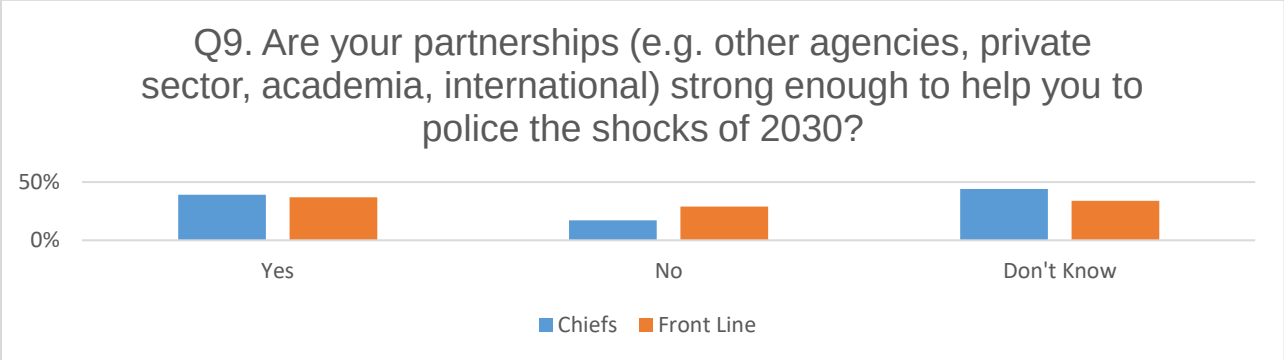
Commentary on Q6

The commitment of resources to learning and innovation was evenly reflected by the Chief Commissioners and Front line members at less than 50%; this may be a significant area for attention particularly when looking at what might be done to better prepare police organisations to confidently react to cyber-crime threats.

Commentary on Q7

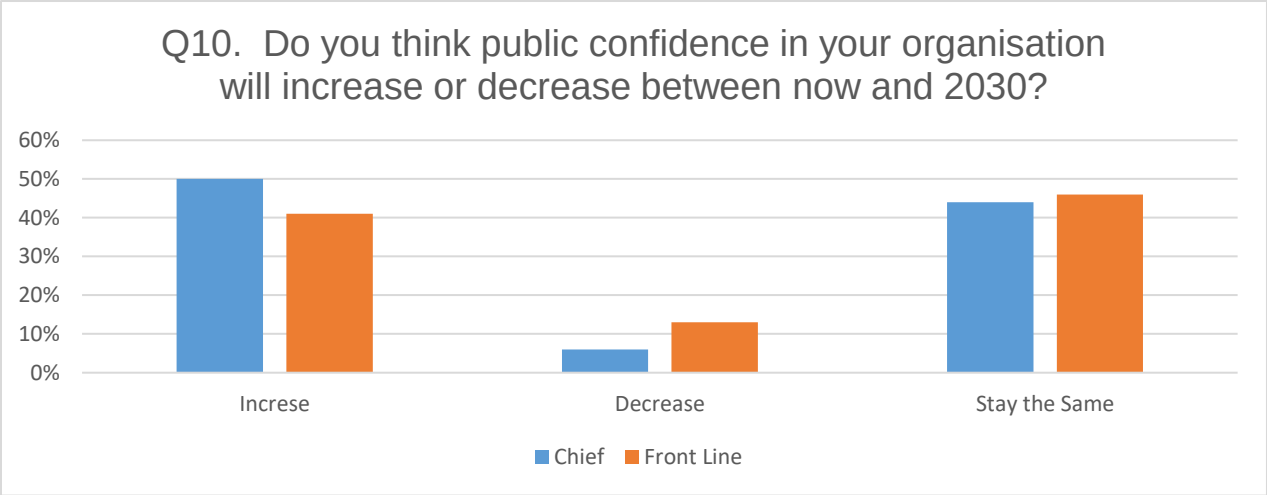
Scenario training to better prepare for future shocks shows a marked contrast in opinion with the Chief Commissioners indicating that just 50% do not consider the organisation practices their responses sufficiently. Front Line members, most probably those members who are the ones participating in the scenario training, voted over 50% that scenario responses were adequately dedicated.





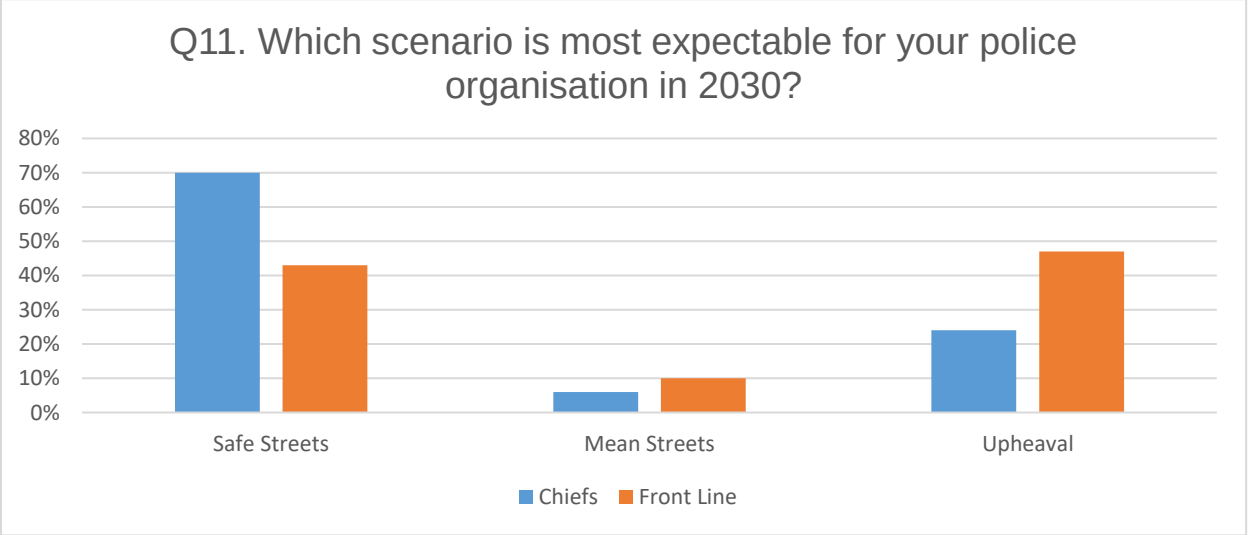
Commentary on Q9

Of note, low percentages were recorded by the Chief Commissioners and Front Line members as to the strength of current relationships as a tool to assist meeting the shocks of the future. There was an uncertainty in the reliability of those relationships and by inference, a nervousness of whether the current investment to build those relationships could be relied upon when required. This may require a revision of who organisations are building the relationships with, how they are being nurtured and if they are being tested in good times to ensure they can be relied upon in hard time.



Commentary on Q10

It is interesting to note that the Chief Commissioners and Front Line members overwhelming indicated that public confidence in their organisation would either increase or remain the same going into the future.



Commentary on Q11

Chief Commissioners indicated that they expected their organisations to end up closer to the Safe Streets scenario than the Mean Streets or Upheaval descriptors. Front Line members however were almost evenly split between Safe Streets and Upheaval which might be an indication of the uncertainty they are experiencing and perhaps a lack of awareness of what the organisation is doing to move to Safe Streets.

3 The Wheel of Shock Resistant Organisations

4 Collaborative partnerships: co-creation of the future

"*We have to abandon the conceit that isolated personal actions are going to solve this crisis. Our policies have to shift.*"
Al Gore, former vice-president of the USA

4.1 Definition

Co-creation of the future through collaboration occurs when cross-sector partnerships are created to find solutions to yet unsolved problems (IALG 2015-2016).

4.2 Connection with police environment

Police organisations are not able to tackle the shocks and threats of the future alone, especially the cybercrime threats. The increased sophistication of international criminals known as "script kiddies", "hacktivists", "cyber criminals" and "nation state hackers" require a different policing approach. We need to co-create the future by combining knowledge and experiences in new ways, being more flexible and agile, as highlighted by the IALG of 2015-2016.

Just as the role of the police has changed, so too have societal roles. Citizens and companies want to be engaged by providing insights and exercising influence. They want to go beyond being passive informers. With today's social technologies, citizens and private companies can be an enormous resource to police work if we build **trust** and include them in our challenges. This will be explored further under the topic of Social Contract 2.0.

4.3 Recommendations

Therefore, a collaborative approach with the public, government, academia and private industry on a local, national and international level, is how shocks need to be managed. This means:

- Sharing and integrating knowledge and experiences
- International collaboration, as cybercrime is an international issue that crosses borders
- Knowledge networks with academics – joint ventures, and the need for a pro-active approach
- Raise cybercrime awareness broadly across businesses and community stakeholders

The following recommendations include specific initiatives to materialise the previous principles.

4.3.1 Fusion Center for Cybercrime

Cyber integrated fusion centers should be developed with integrated information technology, cybersecurity, and cybercrime prevention, intelligence and analytic capabilities. The Cyber Fusion Center is a multi-stakeholder environment that brings together law enforcement specialists and industry experts. These fusion centers would involve private partners, cyber partners, cyber stakeholders, and the cyber community to enhance information sharing processes. For example, partnership with leading cyber security companies, such as Microsoft, Symantec and McAfee, would help police organizations stay up to date on the types of attacks that may affect a policing jurisdiction. The center would work to use innovative techniques and make full use of information available to generate actionable intelligence capable of impacting upon criminal cyber activity in member countries.

4.3.2 Partnership with Academia

Many policing organizations already have partnerships with accredited universities in regards to educating members of the policing organization through adult learning opportunities. Policing organizations should extend this partnership and discuss the possibility of partnering with universities to facilitate research opportunities to assist in identifying innovative approaches to dealing with cyber-attacks and cyber related occurrences. Potentially, this initiative can complement an internship program.

4.3.3 Partnership with Computer Experts

Police organization can offer scholarships and internships to students who are computer experts/white hat/ethical hackers to fill Cyber unit positions (Engineers/ Analysis/ Code Specialist). These individuals are needed to provide an alternative approach to protecting critical infrastructure from cyber-attacks. Their advanced computer skills and knowledge of information technology would be very useful for the police. They can be assigned tasks to engage in penetration testing, provide insights into how to connect with youth as well as develop preventive campaigns which appeal to youth. The most talented students could be offered contract positions once they have completed school program.

(Note: Ethical hackers are IT experts who hack into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent.)

4.3.4 International Framework and Cooperation

Under the auspices, for example of the United Nations, the police community needs to address the issues of impunity, anonymity, access and storage of information, disruption activities and policing the internet. The police and law makers should contribute to the development of the new legal norms and relevant sanctions by creating necessary mechanisms for law enforcement, the judiciary and the prosecution. We also need to encourage international cooperation on a bilateral and multi-lateral basis, in association with international policing organizations such as Europol (Cyber Crime Center - EC3) and INTERPOL (Global Complex of Innovation).

5 Culture of Innovation and Learning

"*Innovation is an essential part of the police organisation*"

Hans Schönefeld, Chief Innovation Officer Dutch Police

5.1 Definition

A culture of innovation and learning is one that is cultivated and nurtured at all levels of the organization and supports unorthodox thinking and its application.

Learning organizations support their employees to take reasonable risks and to learn from their mistakes with a view to moving toward a culture of continuous improvement. Innovative cultures recognize differing points of view and seek out alternative perspectives. Innovation is encouraged at all levels of the organization – and is included as a competency in the recruitment process.

5.2 Connection with police environment

A shift in traditional culture is required in order to create a culture of innovation, learning and transition. A traditional police culture is based on a hierarchal paradigm that values protocol and relies on a reactive attitude to respond to incidents. It is recognized that there is an ambition to change the current police culture and we refer to the strategies below as a starting point for adoption.

5.3 Recommendations

- Build **trust** within your organization:
  - Ensure open and honest communication about the context of situations, limitations, contributions and constraints
  - Enhance transparency, not only under successful circumstances but also when being confronted with problems and failures
  - Be willing to emphasize progress
  - Ensure that there is a commitment to honouring agreements and do what you say
  - Be consistent - act in accordance with values
  - Ensure that successes are visible and allow others to share them
  - Ensure that all people who are involved remain a part of the whole process
  - Be aware of the need to create space for sharing emotions
  - Encourage a culture of seeing failure as an opportunity to learn and grow rather than a "scapegoat" culture

    - Make innovation a part of the requirement to get approval of new initiatives
- Create room for innovation in your organization, by using best and bad practices and encourage individual and collective research in order to enhance preparedness, also for unpredicted and “black swan” events
- Build resilience in your organization through resilience training, supporting members of police exposed to extreme, stressing circumstances and learn from unpredicted and unprepared police incidents.
- Create a lifelong learning environment within your organization – support your staff to engage in learning activities throughout their careers, with a special focus on new developments in cybercrime and cyber threats, by seeking support of academic, industrial and military research and education programs
- Develop communities of practice within your organization related to specific areas and with other policing organizations both nationally and internationally. Initiate twinning – a learning partnership with an external organization – example DEFCON event, a hacking conference the police is able to attend
- Engage in double learning – learning that goes beyond reflection and action and includes reflection on pre-assumptions and basic values.

6 Prevention and Preparedness

"*Embrace the threat – do not be scared but manage it*"

Pier Eringa, President Director of ProRail and former Chief of Police in The Netherlands

6.1 Definition

Prevention and preparedness are related to a professional culture of pro-active risk reduction in order to raise consciousness within organizations and the wider community.

This should be a continuous cycle of events of action, reflection, preparedness, prevention and then pro-action.

This process should then identify vulnerabilities in our planned responses, ahead of shocks taking place and enable adjusted plans to be introduced and then practiced.

6.2 Connection with police environment

The police have a tendency to become overwhelmed when shocks occur through not having planned and prepared for events as thoroughly as they could have.

The police are generally more comfortable in taking action to respond to shocks and then reflecting upon their actions in response to the shocks. What they are less confident with is the deep reflection that is required on future policing and pro-active risk reduction.

At present, police organizations do not practice sufficiently for future shock scenarios. They do not learn enough from other police organizations that have experience of tackling shocks and instead conduct their planning and preparation often in complete isolation.

Currently, most police organizations do not sufficiently engage with the Cyber community and therefore are unable to build **trusting** relationships that provide the requisite support to policing issues.

Being prepared is critical to building community **trust** and supports transparency. It is important to engage the community to create an ongoing two-way communication process – and to engage other professional sectors and government and other stakeholders to ensure that we are sharing responsibility and including perspectives beyond the law enforcement community.

6.3 Recommendations

- In order not to become overwhelmed, police chiefs should pay more attention to pro-active risk reduction in order to become shock resistant.
- Police Chiefs should assess their own capacity and capability to create a culture of prevention and preparedness. This requires an ability to focus on reflection and deep learning with external public and business partners and international policing partners. This also requires capacity internally through introduction of resilience programmes and technological solutions.
- Police Chiefs should create capacity to re-think future policing using scenario thinking, contingency planning and international cooperation in order to increase Government involvement and public consciousness of emerging Cyber threats. This will require implementation of a Cybercrime awareness programme.
- Police Chiefs should increase their engagement with the wider Cyber community to understand their needs and priorities and to explore opportunities for maximizing access to their expertise to assist with policing issues.

Preparedness →	Preventative →		Active →		Reflective
Pro-active risk-reduction	Raising consciousness	Prevention	Enforcement and action	Follow up and adapting	Reflective learning
Scenario thinking Contingency planning Government awareness International collaboration Trust building	Consciousness within police Government acceptance Risk prevention - communities - companies - businesses - citizens - academics	Network analyses Inquiry and signaling Forestalling persuasion Disrupting criminal behavior	Action and repression Limiting effects on society Crisis controlling Victim care Active communication	Evaluation of actions Evaluations effects Rethinking policing Communication Media strategies	Exchange deep learning Networking and exchanging Rethinking future policing

7 New Professionalism

"*Crises preparedness: build emotional ties in good times and the investment will pay off in times of difficulties*"
Rainy Chan, general manager of The Peninsula Hotel Hong Kong

7.1 Definition

For law enforcement organisations to have the ability to manage new and emerging shocks especially Cyber shocks, they have to be supported by "New Professionalism" across a range of Human Resource strategies. New Professionalism requires organisations to be able to recruit and retain people that are forward thinkers and can break the mould of traditional policing to enable to police in a different way.

Shocks are varied and so are the police responses to these shocks. Some require a robust military style response whilst others need a sympathetic and supporting response. Our officers need the flexibility to adapt between these responses and in order to do so they must have personal resilience to withstand the stresses they will encounter when dealing with these incidents. Additionally our organisations must be equipped to provide the psychological and emotional support that is necessary for our officers.

Chris Stone, Professor of Criminal Justice at John F. Kennedy School of Government, Harvard University and former academic on the Pearls in Policing programme has previously advised on the concept of New Professionalism within Policing, **"Professional policing enhances democratic progress when it accounts for what it does, achieves public support, learns through innovation, and transcends parochialism."**

Human Resource Strategies that adhere to these elements and sentiments will enhance the organization's capability and resilience to respond to shocks and will provide mechanisms to look after our staff following shocking incidents.

7.2 Connection with police environment:

Many of the current police organisations have archaic Human Resource strategies, they are too rigid and simply do not provide the required flexibility to adequately equip the police for future shocks, more particularly when it comes to cyber.

Recruitment at the lowest level of an organisation remains common practice along with the awarding of lifetime contracts. A lack of innovative

reward, engagement and empowerment strategies together with insufficient resilience training and personal development opportunities, all fail to enhance internal relationships, diminish our organisational resilience and minimise the loyalty we require from our staff to help us cope during periods of shock.

The Police constantly seek to re-invent the wheel when lessons can be learned from other police organisations and the private sector who have experienced shocks and have implemented the necessary changes to their strategies.

The Police can no longer train their own experts across every spectre of modern day policing and this makes little sense if such skills and experts already exist within the public sector.

The Police currently fail to attract sufficient numbers of potential recruits that have the required academic background to enhance our capabilities within Cybercrime Units.

7.3 Recommendations

- Police Chiefs should review and implement changes to their recruitment strategies to ensure that they provide the flexibility to enable them to recruit people with the necessary skills, for the right period of time and at the right level within their organisations. Increased use of fixed term contracts should be introduced at all levels. The aim is to enhance capability, improve agility and effectiveness when dealing with shocks. This is particularly important when facing new challenges in the Cyber environment.
- Police Chiefs should review and implement changes to how they currently invest and reward their staff. A holistic approach is to be considered. This approach includes financial and non-financial reward incentives, resilience training and personal development opportunities as well as providing a healthy working environment. We have to prepare our staff for dealing with the inevitable shocks and be prepared for providing them with the requisite support both during and after the shocks occurring.
- Police Chiefs should ensure that they are actively seeking best examples of New Professionalism from across the world. Shocks are occurring all the time, reviews are being conducted and lessons learned from these experiences are being implemented in the impacted countries. These lessons learned need to be shared

internationally and acted upon in advance of further shocks taking place.

- Police Chiefs should increasingly seek to utilise experts from the private sector to deliver against tasks requiring highly specialist skills.
- Police Chiefs should engage with academic institutions to develop Cybercrime internship programmes that will provide students with practical work experience in Cybercrime Units and should enable organisations to offer employment to the most talented students.

8 Embrace Technology

"*Cyberspace has become a part of real life and needs a new way of policing*"
Ben Caudron, Professor sociology Erasmus University of Brussels

8.1 Definition

The pervasiveness of technology in society will (if it has not already) mostly disrupt, and sometimes enhance policing. The average citizen is increasingly living in a digital world, relying on algorithms and mobile devices to do everything in their normal lives (banking, telecommunications, shopping, entertainment). The millennial generation are digital natives who might never step into a physical bank or grocery store, instead having these everyday tasks done electronically, on-demand and on-the-go.

The pace of development in this digital age is also unprecedented. The first iPhone was released in 2007 with 800 apps on the Apple App Store. We are now on the 7th generation of the iPhone (with new capabilities unrecognisable from the 1st generation) and with 2.2 million apps on the App Store. Contrast this with our police tech systems which are monolithic structures, that take years to develop the next version.

Organisations (including criminal) are developing fast in using an abusing new technologies impacting considerably on political, commercial, social and criminal activities with more and more impact on each citizen individually and on the society as a whole.

8.2 Connection with police environment

8.2.1 Digital Nexus to Crime

We must recognise that in the very near future, most crime will be a cybercrime (as a target) or have a cyber-component to it (as a tool).

Not only has there been an exponential increase in the absolute number of crime cases which rely on digital evidence, the amount of available digital evidence per case has risen exponentially as well. Police organisations will be overwhelmed. In addition, important cyber-attacks have been notified with more and more dramatic consequences on society e.g. in hospitals in the UK.

8.2.2 Police Organisations are Not Good at Adopting New Technologies

Law enforcement agencies have traditionally been very inefficient and ineffective in adopting new technologies. Development of IT systems and other technologies are often over-budget, delayed and, more critically, do not deliver what was originally intended. Examples include the case management systems from Denmark and Sweden, and criminal intelligence logging system from UK.
Most law enforcement agencies are preparing the future mostly in an isolated way, not taking full profit of similar needs and developments in other law enforcement agencies (both at national and international level).

8.3 Recommendations

- Most police organisations still have a traditional way of adopting technology, that takes years and is based on fixed contracting. We instead recommend having a bi-modal strategy for adopting technology:

	Traditional	**Agile**
Methods of Development	Traditional contracting where there is a fixed scope of work and timeline.	a) Acquiring on-the-shelf and proved products b) In-house development, hiring software engineers c) Cultivating a group of ethical hackers, e.g. DEFCON and Toronto Police Service d) Strategic partnership with a trusted tech firm. E.g. NYPD has a strategic partnership with Microsoft.
Development Turnaround	Years	Months / Weeks
Suitable Systems	Systems for core and stable functions. This includes command and control systems, dispatch systems, blue-force tracking systems.	Systems that have unclear or fast-evolving requirements. This includes sense making systems, tech forensics systems, even public communications systems.
Legal framework	Current legislation is mostly not adopted to new technologies	Creation of sustainable legal frameworks that are technologically neutral

- Create a joint digital platform made up of law enforcement agencies, tech companies, higher-learning institutions. The joint platform could facilitate the scanning of new technologies and contextualising its impact to policing, and the subsequent crowdsourcing of possible solutions.
- Leverage on the digital-savvy officers (permanent or temporary contracts) within the police service, place them in positions where their contributions can be maximised and their skillsets harnessed.
- Identify ways in which to secure new technologies. Implement or influence the necessary policies and legislations needed to minimize impact of new technologies. E.g. define and implement security baselines on all major operating systems.
- Prevent your organisations from engaging to easily in new hypes and non-proved technologies

9 Social contract 2.0

"*In order to deal with the digital world, we need a new social contract*"
Yvan De Mesmaeker, Secretary General ECSA

"***Trust*** *(of authority, government, police) has diminished, offering two options: work to regain* ***trust****, or adjust to the absence of* ***trust*** "
Lui Tai-Lok, Professor, The Education University of Hong Kong

9.1 Definition

In moral and political philosophy, the social contract or political contract is a theory or model, originating during the Age of Enlightenment (especially Rousseau, 1762), that typically addresses the questions of the origin of society and the legitimacy of the authority of the state over the individual. Social contract arguments typically state that individuals have consented, either explicitly or tacitly, to surrender some of their freedoms and submit to government authority, in exchange for protection of their remaining rights.

9.2 Connection with police environment

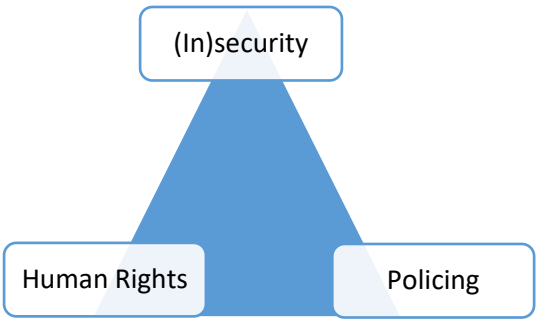
Intensified monitoring of flows and nodes can pose a threat to the privacy of citizens, because non-suspects will also be monitored and surveyed simply because they are moving within a particular flow. However, citizens might accept this intrusion of their privacy, because it prevents them from being subjected to other kinds of instruments that would infringe on their rights and privacy even more. In other words, these controls are reasonable. Citizens therefore need to accept that the expansion of some police powers counterbalances their ability to move around freely and safely. There will always be a tension between protection by the government and protection from the government; the right balance is not static but shifts and adapts along with the societal context. Public consent for policing has evolved gradually over decades but rapid developments in digitalisation and the online environment mean that there is less clear consensus in these areas.

Especially during and short after shocking events, the public is ready to accept extraordinary ways of policing, be it to support people in dramatic circumstances or to take a robust attitude in order to prevent even more dramatic impacts. This requires from the police a situational and flexible response bringing the police leaders and members under extreme, stressing working conditions although they are not always prepared to maintain a sufficiently resilient attitude.

The consequence of all this is, that the classical social contract theories not immediately fit immediately for the often unprecedented situations. Although the public is ready to accept new ways of interacting between the police and the people subject to these situations, the police has to make sure that they do not breech the so needed **trust** once things are brought back to normal.

9.3 Recommendations

- Within the framework of the society they are policing, police organisations must find a balance between the level of security one wants, the respect for human rights and the way in which policing is done, especially during and after shocking events and when combating cyber crime.



- Therefore police organisations must educate and partner with community and civic organizations to co-create a common ground of the purpose of law enforcement and encourage community support, with a particular focus on the digital world. Police organisations must continue to 'lead by example', even under extreme conditions, by respecting the evaluating and social legal framework themselves.
- The collection of police data has a huge impact on the respect of privacy in society. Collection, use and retention must be subject to regulation, supervision and accountability to reassure the public. The collection, use and retention of police data should be adequate, relevant and not excessive also in pre, during and post shocking circumstances. As discussed in 2016, the limits of policing (under- and overpolicing) have to be well defined in order to design a global framework and the limits of policing when building shock resilience.
- Police professionals and citizens co-create a mutual understanding about balancing the rights and responsibilities in society and collaborate together in societal security with a particular focus on the eventual exceptional conditions related to above mentioned events.

Special attention must be given to the time and space dimension for which society is ready to accept exceptional ways of policing.

10 Future visioning

"*The future is not what you will expect it to be*"
Moodi Mahmoudi – CEO Collaborne.

10.1 Definition

To cope with the future is to deal with uncertainty. It ranges from known-knowns to unknown-unknowns. In rather stable, meaning simple and complicated environments the future can be surprisingly predictable. Stable interactions make it possible to know what is going to happen. In dynamic, meaning complex and chaotic environments the future can be predictably surprising. The dynamics will result in unforeseen outcomes and relations, or even complete surprises.

Problem statement: how to predict the future? How to promote your preferred future (policing the future)?

10.2 Connection with police environment

As already discussed during the Pearls meeting 2007-2008, the ability of most police organisations dealing with future visioning is not very mature. There are rudimentary efforts in using big data, and a constant scanning of future developments is often an exception.
Predictive policing is the exception, reactive policing the rule.
Visioning in a policing context should focus primarily on threats and (probable and possible) risks and should include information, organisation and culture/attitude.
It is essential to involve scanning, forecasting, foresighting of new developments in the world and societies, to use more the concept of scenario thinking (societal and organisational) and to experiment unforeseen and unprepared events.
Forecasting has to rely on the use of data-analytics (big data, algorithms, etc.) It will be most effective in environments with more or less stable interactions.
Foresight can be used in the complicated, complex environments. It will focus less on data, but more on the use of images (storytelling, scenarios, etc.)
Experiments can be used in complicated, complex environments, especially in situations where there is little time/space for interaction.

10.2.1 Cyber

The exponential development of the digital world, especially cyber, has and will continue to have a huge impact on future policing. Examples are the use of darkweb and encryption on investigating cybercrime. Other are the misuse of 3-D printing, self-driving cars or the 'internet of things' that bring challenges to security.

10.2.2 Shocks

Each police organisation has to be prepared for shocking events. Dealing with shocks includes:

- Absorbing the shock in a robust or resilient way. This will get the organisation back in the old state.
- Acting in an agile way (i.e. avoid the shock)
- Acting in an anti-fragile way (embrace the shock, benefit from the unexpected) will lead to a new state of the organisation.

This requires an attitude of constant scanning or even productive paranoia.

10.3 Recommendations

- incorporate the process of future visioning in your organisation
- create a culture of **trust** where productive paranoia and constant scanning of the environment SUSTAINS
- invest in the possibilities to effectively use forecasting, foresight, experimenting and scenario thinking
- police the future: influence developments in societies from a security/policing point of view
- make sure your organisation is able to adapt to surprises/shocks in the quickest possible way without harming the **trust** of the public

All of this may very well include the use of (sustainable) partnerships (quadruple helix i.e. government, private sector, academia, citizens).

11 Transformational Leadership

"*To survive in a radically changing environment, we have to modify the DNA of the Police"*

Henk de Jong, Director of Strategy Dutch Police

11.1 Definition

The globalization brought a lot of benefit to the world. Exchange of knowledge, information and products without borders almost real time to every angle of the world has become quite usual.

The digital transformation in our society is one of the biggest drivers in that process. The impact on our society may be bigger than the industrial revolution during the 19th century. Therefore, transitional leadership is becoming the predominant leadership style for organisations being by definition interconnected with society at all levels.

11.2 Connection with police environment

Transactional and authorative leadership have traditionally dominated law enforcement. While attitudes are changing and these approaches are slowly losing their appeal in favour of transformational leadership, building resilience, especially when being confronted with shocks and cyber threats, needs to be brought in by the current police leaders to implement organisational change in order to increase shock resilience. This means that transformational leadership can help an organisation to be resilient by being more innovative, caring, visionary and inspirational, and to build **trust** within the organisation and the public they serve.

11.3 Recommendations

11.3.1 You as a leader have to embrace shocks!

That means:

- **trust** and empower your people
- clear boundaries of responsibility
- create a no blame culture where decisions have been made in good faith, with sound rational and with protection of the public at their core, especially after having been involved in shocking experiences
- share lessons learned to prevent them of being repeated
- implement good ideas
- have a checklist of improvements in your pocket for the post shock period

This means, that transformational leadership should lay, whenever appropriate, the fundamentals for a more situational leadership approach when managing crises or other shocking events.

11.3.2 To build an organisation which is prepared for cyber shocks you need to focus on transformational leadership.

A transformational leader (style) is defined as a person (style) within an organisation who is visionary, innovative, inspirational, and sensitive to the needs of others.

That means:

- articulate core values about cyber
- build vital coalitions
- involve the outside world
- organize teamwork and **trust** building
- appreciate contrasting perspectives

11.3.3 The need of a transformer

Ideas that will affect the DNA of police forces are difficult to implement. Therefore you need a transformer: a person that keeps the focus on future visioning and shock management. This person's skillset comprises:

- a leader that is a dynamic individual to lead a team
- facilitating transformation within the organisation
- including a team of leaders having the appropriate skills to manage different concrete situations
- embracing shocks as an opportunity to transform
- having a high profile within the organisation and willing to influence government policy, procedures and legislation to prepare the organisation for future shocks.
- leading high profile media campaigns

12 Conclusions on the assignment

Police organizations need to:

- Develop a culture of future visioning, innovation and learning, welcome and embrace new technology. Use cyber as a vehicle for change, the ultimate goal is to get your police service /organization to the desired “safe streets” state.
- Prepare for the unknown and anticipated threats. Collaborative Partnerships, New Social Contract, Contingency planning will therefore be part of the process of making Police organizations resilient. The DNA of the Police has to change at all levels to enable your organization to implement the wheel for shock resistant policing organization.

Trust and **building trust** are keywords.

13 Reflections on the IALG

Along our journey we encountered a few challenges:

- The difficulty of testing a new platform “Collaborne” while working on the assignment. It was helpful in collecting data. However, it could not be used further in the process and did not produce a final presentable product.
- The assignment brought two questions in one, which made it difficult to approach.
- There was not sufficient time for participants to combine their work and the demands of the wickedly difficult assignment.

14 Recommendations

- The program management might consider to bring in more geographical diversity in the selection of IALG participants by bringing in participants from other continents.
- More continuity between and implementation of outcomes from former IALG assignments could be considered.
- The academics ought to be brought in earlier in the process, to work with the participants on the assignment. Bringing them in the second week would have been very helpful.

- The IALG is of the view that the conversation that has started between members of the Pearls group on the topic of creating a shock resistant organization with a particular focus on cybercrime, ought not to end with the conclusion of this conference.
- With modern communications and social media as a focus, we have taken the liberty of creating two secure, private and by invitation only groups on both the Linkedin and Facebook platform. These two platforms are two very large and very mainstream platforms that are most appropriate. We have on file all of your work email addresses. With your permission, we will activate these groups in either the Linkedin or Facebook platform so that you can continue this discussion both securely and privately. If that is the will of the Pearls group, please expect to receive an email inviting you to become a member of this group. The only questions is to identify your preference, Facebook or Linkedin.
- We suggest the following topics for next year's conference:
  - The development of an International Fusion Centre for Cybercrime as is suggested in this paper.

This takeaway booklet summarizes the recommendations that have been provided to you and might be a good reference and starting point for the next steps or way forward into your organizations.