BREAK OUT!

LIVING IN THE NEW UNREALITY

Colofon

Graphic design: Zilverster-media, Annelies Dollekamp
ISBN 978-1-4457-7966-9

BREAK OUT!

LIVING IN THE NEW UNREALITY

Huub Stiekema

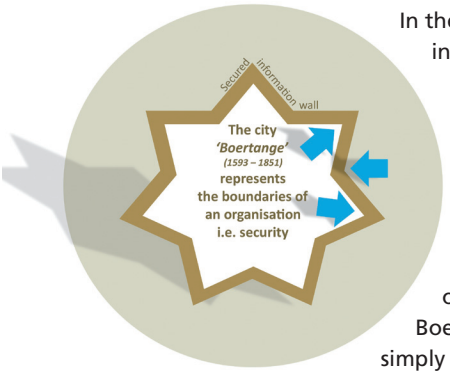
The new reality

Now you are the voice
You will lead not follow
You will believe not doubt
You will create not destroy
You are a force for good
You are the leader
Defy all odds

Set the new reality

(based on A. Robbins, Rome 2009)

FOREWORD



In the Spanish war, Willem van Oranje ordered in 1580 A.C. the building of a 5 star shaped defence wall around the city of Boertange in the Netherlands. The only way in or out was via a narrow sand path through the swamps. While this afforded good security, it also meant that the citizens of the village could not easily trade, work, live or play with the citizens of other villages. In reality the city of Boertange was not secure at all. It was simply isolated.

Society in the industrial era is based on mass production, mass distribution, mass consumption, mass education, mass media, mass recreation, mass entertainment and mass destruction. Combine this mass orientation with standardization, centralization, concentration, and synchronization, and the basics for the current bureaucracies are shaped; it's society, as we know it.

Society now is at the crossing point of two eras: from industrial to the information era or economy. In the industrial era management gurus like P. Drucker (Austria), M. Porter (USA), C.K. Prahalad (India) and A. Toffler (USA) defined the corporate structures, as we know it, but also predicted the current information era by defining ingredients of change because of the use of information. The current post-industrial society with a polluted earth, a devastated environment, a broken economy and a fragmented humanity are the chaotic remains of the past industrial era and the beginning of the information economy, where the old boundaries will break down. The Industrial Revolution has cost us more than it ultimately delivered. Society has to turn – is already turning - the bow of the ship to use information as a new resource to come up with bright solutions to create a better world. The tools of the new era are sophisticated digital communication technologies. They are being used by the best semantic processors on the planet; you and me. The information era becomes a global network structure facilitated by Internet technology. Today, mass-adoption of information and communications technology is breaking down corporate structures and boundaries and creating new horizontal structures: people and businesses interacting with each other across pre-existing business and nation state walls. Social structures and new technologies are therefore influencing the way people live and interact.

The Internet has enabled a 'mass-breakout'. There are many societal and economic benefits to this, and there are also new risks and threat levels.

Criminals use the new information technology too and have created a whole new 'line of business' based on new technology. Information can be worth a lot of money and all kind of social, and industrial structures are based on the use of information and technology. Criminals can harm society seriously by using traditional and modern technology.

Since the modern police service was founded, it has always adapted to the changing environment around it; not as early adaptor, but as true follower of societal changes. Police organizations are bound to criminal law and criminal procedures and therefore are used to reacting to societal developments. The question now is not if, but how and when, will government in general and specifically the police organization adapt to the mass-breakout and step into the outside world and its technologies. Understanding this outside world is essential for police management and its administration. This transformation brings along various paradigm shifts for society and for police organizations. The grand question therefore is how, when and by who, will upper police management assess current paradigms around internal and external communication, collaboration with partners, openness or sharing information, the usage of modern technology and positioning innovation, in order to enable next policing to grow to 'serve and protect' in a human-digitized world. This book is one of the scenarios of doing police work, 'next policing'.

The concept of next policing is a vision to a new form of executing police work in the near future – our current reality - based on using information, intelligence, technology and new ways of collaboration at the centre of the vision. It is not about policing scenarios in the world in 2025, because not only is that the ground of 'Pearls in Policing'[1], but the new reality of mass-everything is the reality of now also. Next policing is about the change of the fundamental paradigms of the police organization given emerging information and communication technologies, which will have a deep impact on communication and collaborating patterns between people, organizations, scientific institutes and … criminal behaviour. Because of that and the inherent information dominance, police business as it is now, is history; business as usual doesn't exist anymore.

From a corporate information technology perspective international companies and governments have been very busy investing in large data centres around the world. A key goal was to deliver secure data with highest integrity against the lowest cost possible. Billions of dollars were spent on standardisation of information technology in a traditional 'record keeping' way. But did it deliver up to the promises? Or do we now see that there is a big leap between constraining end-users by corporate information technology governance and, supporting end-users by highly collaborative Internet functionality and open

source data. By far the most demoralizing decision from government's upper management is to prevent their employees to work with the Internet out of fear of the unknown. By that statement management expresses to the company that they don't understand this movement, society, colleagues and the new forms of collaboration and the applications they use. In a negative explanation management sends out a message of mistrust and misunderstanding. From an information technology perspective the grand question is how to facilitate both the 'black wire' and the 'white wire', i.e. the corporate local area network and the Internet.

This book doesn't give all the answers, because future questions are not clear. It gives insight of the digital society and a few consequences of a digitized society in which we live. The book doesn't contain the truth, but intends to initiate several discussions amongst professionals and strategic management. If strategic management decides to put aside the underlying messages, then, for sure, the impact of the information era on the police organization is not foreseen and the business will dramatically fall down in performance; professional criminals will certainly use the new technology to their benefits.

Whatever the outcome of strategic management, I sincerely hope the police manager reading this finds the help to step into the 21st century. After reading this theory the police manager maybe transformed from the "TV-generation" to the "Gaming-generation" and so has a clear vision that the network and information dominant society is the society he has to 'serve and protect'. The police manager is connected to ideas and common understanding of what happens in modern technology and, more importantly, modern communications. The police officer can transform himself from a passive viewer to an active participating decision maker that would likely to make him a better police officer as well.

Unfortunately most professionals are confused too, because there is no clear direction. An important suggestion is to use the Internet more frequently, to look for new experiences and to initiate the discussion internally. For that purpose I have set up a Dutch Internet site for police business, Intelligence, technology and mass communication (http://www.politie2.nl). You are warmly invited to be a part of that community and share knowledge of modern technology and communications, and also to mingle in the discussions on the Internet about your business. The adage of this community is: 'we know more than I do'. You can also follow other discussions via Twitter, by following 'policetribe' or see some real cool stuff on YouTube.
The title of this book: 'Break out!' can be taken literally. Outside of work people are already living in the information space - the new reality. It's the reality of

the criminal world, it's the reality of their home situation and the very people the police is working on to protect and serve.
But, when the police officer goes to work he puts the corporate-'4 walls' around himself; he puts his uniform and weapons on and he is using the internal 'black wire' corporate information stream only, protected by a strong internal firewall. He emerge himselve into a 'bubble of unreality'. But how can he continue to, 'protect and serve' those who need it the most? Although I realise that this is one, and perhaps my, reality, it is still the context and the big question I give the reader to consider.

Finally I'm sure of one thing and that is that 'intelligence' rocks and the Internet is not a hype. It is the key element for police business to grow into the next century. It will be the next and exiting era in human behaviour.

Huub Stiekema
Business innovator

---

[1] An international cooperation between national police forces to foresee the future of society and with that future policing.

ACKNOWLEDGEMENTS

Before I start I would like to thank a few colleagues, friends and loved ones who helped to get this book written. I have loved and appreciated the professional discussions with my dear friend Carl. Carl has been a tremendous source of inspiration to me for the past years. As highly skilled boardroom advisor he is able to simplify difficult matters, give direction and take result driven action. He is the main reason why this book is in English and he promised me that if the book becomes a bestseller, than he is going to translate it to Dutch. I cannot wait to see that happening.

Thanks to Leon, Ruud and Wim for their professional reviews. They are innovative chiefs of police in the Netherlands and they put a lot of energy in important business developments like business architecture, information strategy, technology for crime detection and crime prevention and Internet enabled platforms for collaboration and communication between police professionals, like: IPEP: www.ipep.info.

Furthermore I would like to thank Jacques, Silvio and Marga for their excellent comments and reviews. These colleagues are drivers for continuous improvement of the police organization, information technology and Internet initiatives like: www.politie20.nl. They are pushing barriers all the time and are not afraid of taking project risks in order to get it done.

I would also like to thank Henk and Henk. The first Henk leads a strategic analysis department. He is the most intelligent of all and he has challenged me for the last years on bringing back my far away concepts to the reality of today; a valuable asset in every organization. The last Henk is somebody I met several years ago, but learnt to know better just recently. He is very knowledgeable on the history of the police. Because of him I now understand more of the hesitation of any police officer to share data and to enter the digitized world.

I would also like to thank Marcel. He is a brilliant information and ICT architect and somebody with whom I can challenge almost every thought, direction or vision. He also became a close friend and tought me about the value of the Internet. He still is an inspiration for me to come up and execute new initiatives.

Before I really close these acknowledgments I would like to thank my dear wife Yvonne and daughters Kim and Marit for their patience and moral support.

It took a while, but *Break out!!* finally hit the (digital) book store.

Thank you all.

CONTENT

Table of content

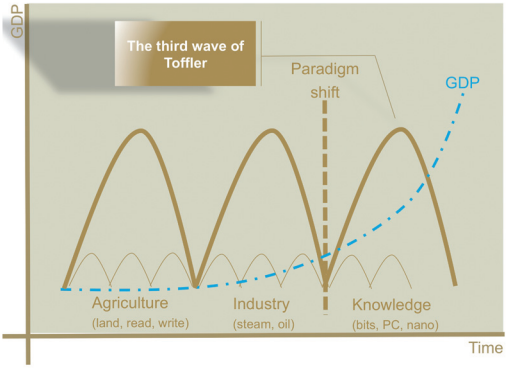
FOREWORD	6
ACKNOWLEDGEMENTS	12
TABLE OF CONTENT	14
PROLOGUE	16
CHAPTER 1 THE BIGGER PICTURE	22
CHAPTER 2 THE INTERNET SOCIETY	36
CHAPTER 3 THE INTELLIGENCE FLIP	58
CHAPTER 4 POLICING IN DIGITAL SOCIETY	80
CHAPTER 5 THE MODERN POLICE ORGANIZATION	94
CHAPTER 6 IN SECURITY WE TRUST	114
EPILOQUE	130
REFERENCES	136

PROLOGUE

Shifting paradigms

Alvin Toffler (born October 3, 1928) is an American writer and futurist, known for his works discussing the digital revolution, communication revolution, corporate revolution and technological singularity. His early work focused on technology and its impact through effects like information overload[1]. He moved to examining the reaction of, and changes in, society. Technological singularity is a term related to super intelligence and in the predictability of the future and accelerating change[2]. In 1965, I. J. Good first wrote of an "intelligence explosion", suggesting that if machines could even slightly surpass human intellect, they could improve their own designs in ways unforeseen by their designers, and thus recursively augment them into far greater intelligences. The first such improvements might be small, but as the machine becomes more intelligent it would become more intelligent, which could lead to a cascade of self-improvements and a sudden surge to super intelligence. Toffler also states, in 'Rethinking the Future', that: the illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn.

Society became industrial and was based on mass production, mass distribution, mass consumption, mass education, mass media, mass recreation, mass entertainment, and mass destruction. If one combines those things with standardization, centralization, concentration, and synchronization, society winds up with a style of bureaucratic organization. The third wave is the post-industrial society and society is at the beginning of this wave. A polluted earth, a devastated environment, a broken economy and a fragmented humanity are the concrete remains of the past era. The industrial revolution has cost society more than it ultimately has delivered. Society has to turn the bow of the ship. The tools of the new era are sophisticated digital communication technologies, which connect humans. These new technologies make it possible to transform to a network based society. A society where everything and everybody is connected and a society where people and businesses live and work together with their environment. The third wave society was described in many ways: super-industrial society, the information age,



the third Space, space age or scientific-technological revolution. In various degrees the terms described de-massification, diversity, knowledge-based production, and the acceleration of change: "change is non-linear and can go backwards, forwards and sideways". The linear, mechanicistic, business processes must be much more like a network of interconnected activities. The nodes are intelligent people and machines. In this post-industrial society, there is a lot of diversity in lifestyles with subcultures, adhocracies shown in fluid organizations, which adapt quickly to changes. Information becomes the main material for workers who are loosely affiliated. Companies must redefine themselves. The survival of the fittest is not 'fighting alone against the bad outside world'. It is about adaptability and change. Companies that continue to thrive on their past beliefs will not survive the transition. Think of how people today book a trip abroad, close insurances or buy a book or music album. Consider a site like 'Eventful', taking fans to their favourite artist where the fans can indicate where they like to see their favourite artist play. The fans in question determine the location of the company behind the artist.

Society is already undergoing a transformation with different paradigm shifts. Society transforms from an industrial, or pre-web, era to an information and knowledge economy. This means that global progress will not be delivered by traditional developments within a commerce or whole branch of activities, but will be delivered across organizations through information sharing and information recreation. This is a profound change, but in itself not a new phenomenon. Changes, smaller and bigger, are of all times. In fact one of the most important founders of our democratic state stated.

> Will we dwell in what our forefathers bestowed on us, will we not do anything ourselves, will we resist timely advance, well then, rather than advance, we will face decline. Each era has its own principle of motion; if one lets this lie, the following era will suffer commotion.
> **Thorbecke, 1872**

In fact it means that each generation gets its own share of developments, shifts and changes to address and needs to adapt to these changes. Looking at police organizations, their mission statement is *'to protect and serve'* and one of the most important articles of the police law is: *'to help those who need it'*. If police organizations throughout the world are willing to keep their promises to society, it's evident that they must move their organization into the information era and follow through their strategy.
The social -, demographical -, technological borders change at a rapid pace. The shift from local to global, the intensity, rejuvenation, digitization and hardening of crime and social misbehaviour, the invisibility of crimes due to the Internet

and the collaboration between the so-called underworld and legitimate business people are symptoms of this trend.

Re-evaluating the position of the police in society is constantly necessary. Internationalisation, safety value chains, service orientation and virtualisation are new ground rules for this evaluation. Obviously it will lead to new insights in civilian's expectations and necessary products and services to be delivered to the public. In re-evaluating the police as part of society it is obvious to re-evaluate society itself as the dominant partner in the value chain for safety and security.

Collaboration between partners in the safety branch or between the safety branch, science and private companies will also change. The traditional forms of collaboration will be challenged by the notion of fluidity and the light speed of change. In the private sector, companies extend their borders by cooperating on a professional and information centric way by building 'mashups[3]'. Traditional borders disappear in favour of potential growth of the industry, using the crowd. This requires flexible business processes, an open mind of top management and matching policies around information exchange. Internal management controls and process optimisation is no longer enough by itself to work in the new external environment of connectivity. What skills are needed in the police organisation to embrace the opportunities and manage the risks of global connectivity?

The impact of digitalisation on society is phenomenal. The playground is a global community of 2 potentially 3 billion people connected to the same network, using the system without any training or manual. Nobody knows what will change, in what direction and how quickly. People and machines become fused, in the future all physical things will have a sensor that receives and transmits signals of all kinds. Because of connectivity everybody can have the same information. To put it stronger: those who can access information easily are tomorrow's world leaders. Across barriers of time, distance, location, language people will find new forms of collaboration and business leaders will need to adapt to this change.

Information and communication technology is no longer an enabler of business, but a key business driver. In future people will solve the traditional barrier between business and IT; because IT will be business as usual. The Dutch police is now working on implementation of the current Information and communication technology strategy: 'Het Wenkend Perspectief[4]'. This will be the foundation from which the police will have to jump to the strategy of 'next policing'. This strategy is defined as the strategy in which the organization is led by intelligence, collaboration with partners is seamless, the Internet is the core of the information

strategy, open source intelligence is business as usual and the issues with information security are lifted to the next level.

Apart from all these changes, the police play an important role in public safety. In order to properly fulfil and professionalise that role in society, the police must listen to society and think of methods of how to adapt to these current changes. In these changes information and technology play a very important role. Not only a specific community is of interest for the police too, but also the information, goods and persons moving from one community to another. These spaces of flows[6] combined with light speed technological developments and a global connected network, sets the scene for the police in the near future

The mission statement, *'to protect and serve*[5]*'*, needs to be re-challenged against the developments ahead. So apparently, this book is about the police, but in fact it is not! It's about the way and speed the police have to adapt to these major changes and get involved in this *'new society'* again. To serve the reader, the book will not describe every aspect of the police organization. The main focus is on the intelligence and technology function, a modernisation scenario for the police organization and important 'open' issues like: privacy 2.0, security 2.0 and transparency 2.0. Because whatever the changes may be, people still have the utopian longing for maximum safety and maximum freedom.

I hope you will find that this book will take you by the hand. First to give some insight in the bigger global change. After that the book will focus on a new kind of society, namely the Internet society. This is a *'glocal*[6]*'* society based on new principles and values. It's a society in which most of us will live the next decades. The book elaborates on the police function, the Information and communication technology function and the change both have to make to live up to the societal promises. After insights of the Internet society the book will feed the reader a new concept: 'the intelligence flip[7]'; rethink intelligence intelligently, what did intelligence look like in the pre-web era and how can it be shaped in future? Put everything you know about intelligence in an open world and 'open source intelligence' is created. This book explores the issues of information security, trust, transparency and privacy in the context of the same information space. After this journey through information space you will have a notion of the most important building bricks for a modern police organization. And believe it or not, it will explicitly not be an extension of the current organization. It will be a complete and fundamental restructuring of the organization; its societal position, structure, strategy, intelligence, business processes and external collaborations. Finally you will be confronted with the new unreality: *'the police organization finds itself in a new unreality in the connected society'*. The grand question is: if this unreality is true, where did it originate from and how can we get out of it?.

Changing is not a new process for the police, in fact it is continuously changing due to societal, technological, criminological and legal changes. The police organization had always adapted to new situations. However, the speed of this change and the global size of this change will challenge the capabilities of the organization more than ever before. More important than the change itself is the meaning the police organization gives this change and the actions coming from this. We all know that society is in a transformational state towards the information era, no question about that. Many people went through all kinds of societal changes and this change is not different from the ones before. The meaning the organization gives this transformation is in fact the interpretation of the paradigm shift at hand! So in order to foresee and steer the organization into the future, strategic management must identify, redefine and reset existing paradigms by challenging the current rules.

These are not conclusions, because conclusions mean the end of the discussion. And this doesn't suppose to be the end of the discussion, but merely a trigger to start the discussion amongst leaders, management and colleagues about transformations, paradigms, Internet strategy, collaborations and the benefit of this for society. After reading this book I hope you find it would be valuable to ponder on the effects of that profound change in the police organization and to have at least one discussion about this subject in your organization.

> "A self-organized system must be always alive and without finalizing, since conclusion is another name for death."
> **Stafford Beer, 1970**

---

[1] Information overload is a term which refers to an excess amount of information being provided, making processing and absorbing tasks very difficult for the individual because sometimes we cannot see the validity behind the information

[2] Accelerating change is an increase in the rate of technological (and sometimes social and cultural) progress throughout history, which may suggest faster and more profound change in the future.

[3] A mashup is a web page or application into which data from multiple sources are combined and presented together. In organizational terms it means that the clear industrial boundaries between two or more organizations become vague and transparent

[4] Kuijs, Schonfeld, Stiekema, 2005

[5] Mission statement of the Dutch police. In other countries a local mission statement applies

[6] The term 'glocalization' originated from within Japanese business practices. It comes from the Japanese word 'dochakuka', which simply means global localization

[7] Bate, Stiekema July 2009


1
THE BIGGER PICTURE

Chapter 1

Since society lives in a global information hub and policing is allways a part of society, it is inevitable to contextualize a few global developments. Local developments can then be placed into perspective of global changes; the term ‘glocal’ applies. It covers the technological changes and the impact it has on society as we know it. Information availability is not territorial but global to an increasing public; criminals and terrorists included. It is increasingly available for the public and people step into the information age; society drives that with the Internet. The Internet is the technological backbone of this massive change. It is a new threat and it provides also a cure. It’s therefore necessary to redefine paradigms and shape the new future for a police organization pro-actively.

Look at the near future of 2025 and focus on the bigger changes. The international arena will change dramatically due to a growing population, emerging powers, a globalizing economy and the transfer of economic powers from the west to the east and an increasing influence of non-state actors. Non-state actors are global businesses, tribes, religious organizations and large virtual networks. The networks can be valuable and peaceful, but can also be very dangerous in terms of terrorist networks or global networks with people intending to do harm to society. The process of building non-state economies is called 'horizontalizing' the economy.

Asia, Africa and Latin America will account for the growth of the global population; the west will increase its population with less than 3%. The number of migrants towards privileged countries will increase and the demand for food will reach critical proportions. New technologies will have to find solutions for those threats in the next two decades. The demand for energy will increase due to the growth of global population and the fossil energy stocks decrease. New technology such as solar energy and wind based energy sources must be put in place.

The transfer of power to the East is not unprecedented. Other global power shifts have occurred in the past. This shift though derives from two sources. The first source is the increased oil demand and the oil prices generated profits for the Middle East and Russia. Secondly, the lower labour costs combined with government policies will shift manufacturing and service organizations towards Asia. With that background China will be the world's second economy and have one of the strongest military global forces. India will continue to be a rapid growing economy and Russia has the potential to enter the global platform again if oil and gas prices remain on the same level as they are now. The political and economical powers of Indonesia, Turkey and Iran will increase also, but without matching the three mentioned economies.
In general the global complexity increases as new players arrive on the platform and existing big players, like Russia, have the opportunity to be revitalized. The multiple actors around the world will change current order in which people cooperate and they will destabilize the international scene and with that challenge international society and social security.
Non-state actors such as terrorist networks, or in general social networks as we know them will continue to grow and influence the world more than we know today. Today's economies have 'vertical' governments and business structures. These vertical structures move towards horizontal structures based on information, knowledge, social behaviour and common interests. At this moment MySpace is in the top 10 of largest countries, if we would treat MySpace as a normal country. These very large networks will influence social -, economical – and political

structures, as we know them now. The only precedent in the past of the same magnitude is religion. Religion has always been a horizontal structure above society; it was divine. One recent example of that is the political instability in Iran, which is fuelled by Twitter as a social network technology[1]. These large digital networks are inhabited by so-called *'netizens'*[2]; people living on the web.

Information and information technology is the fuel for this global transition. Information is anywhere and available anytime to anybody. This will be the final end of the industrial era and its paradigm. Society needs a paradigm shift and is in the middle of the transition towards the 'information society'. Not only can businesses or governmental departments initiate 'bigger' things, so can individuals. The 'old' structure has to react to that development and the professional consumer, or *prosumer,* rises. The global transition requires a new global language; a language of communication and collaboration.
It turns out that the internal facing view of the world is the very thing that now prevents society from understanding connectedness itself. To put this in terms of communication, the specialised language people use in each of our industries gets in the way of understanding the new modern global view; if that isn't an utopian itself. As disciplines and cultures collide, cross-discipline language becomes critical. The new norm requires new language. Here, 'systems thinking'-techniques and next practices are starting to help, allowing us to share a bigger view.

New technology will influence safety in general. New crimes and new methods will emerge, not instead of old ones, but in addition to old crimes and old methods. Public safety will be more complex than it used to be. Cross border crime is not new, but cyber crime is relatively new and almost non-existing in international laws, although it becomes an existing form of criminal behaviour more and more. Child pornography is not a new type of crime, but very difficult to take care of in crime prevention and crime fighting due to relatively young (inter)national laws. Criminal files are no longer on the owner's computer, but scattered around in the cloud and therefore difficult to get a grip on with national laws only. The Internet facilitates that and non-state actors rise. Authorities must deal with new digital criminal activities like 'phishing' and 'farming', which are added to the criminal palette due to the rise of the Internet.

Effectuating the term 'glocal' it is good to consider some trends in a bigger Dutch city as an average of developments in similar cities all over Europe. This city has been the most criminal city in Holland for consecutive years.

THE NEW URBANITE, GLOBALIZATION
Currently it is a knowledge center. This knowledge center is important and one of the largest of the Netherlands. Globalization however may change the position

of the city in that respect. If the city can remain its competitive offer, than there will be brain gain: many highly educated people, both Dutch, Europeans and people from the rest of the world, come to the city to work. But if the city loses the battle, there be a brain drain; *an exodus of highly educated people.* Given that there are 100+ nationalities, living in this city, ethnic and religious tensions elsewhere in the world can cause reactions in the city itself. The "far from my bed" – show doesn't exists anymore. An example is what happens globally with Al-Qaida and locally with mosques and extreme religious imam's.

DICHOTOMY

There is a growing gap between a social group working in society and a social group more or less outside society. The accumulation of problems in these vulnerable groups plays an important role. Financial problems with alcohol or drug use, crime and unemployment caused by a difficult entry into the labour market, for example. Moreover, these groups don't have the right network to independently cope with the problems. The option to get support from the government are often not known or not used.

POLARIZATION AND RADICALIZATION

Radicalization of Muslim youth continues unabated. The growth of Salafism, an ultra-orthodox Islamic movement, undermines the Dutch society. With that trend, the terrorist threat is not immediate. More and more young Muslims deny the challenges and benefits of integration and democratic values. This creates polarization and tension among peoples. Fortunately every action has its own reaction so that the rise of Muslim extremism is balanced out by an internal counter force.

RELATIONSHIPS CITIZEN-GOVERNMENT

In recent years and decades, the role of government changed. There is a receding state, where more traditional government tasks are left to the market or other private institutions and citizens are asked to be more responsible for their own actions. At the same time people's expectation in the government rise, risks are not accepted and people are making great demands on public services. Although the services of the government have improved, these improvements fall short of the expectations in this regard. The above combination makes people trust in the government decline.

IMPROVED TECHNOLOGY

The developments in technology follow each other quickly. Only ten years ago a few people had access to the Internet; in the present societal life there is no way not to use the Internet. These trends introduce rapid changes, including in the field of criminals, the role of government in law enforcement, crime fighting

and expectations of people in society. Moreover, a shift seems to take place in the opinion of the citizens therein. The young generation of the 90th is less concerned about the concept of "Big Brother is watching you" than the older generation.

The developments in our information society accelerate and provide change. Changes in the way people treat information, communicate and work together and, last but not least, changes in business processes and business models in a way that companies can expand worldwide.

The increased and rapid grows of new functionalities and the speed of digitization and technological opportunities mark society, the eco-system and the behaviour of people. Access to information is almost unlimited and independent of location and time. Besides the actual environment virtual worlds are created where it is easier for criminals, not only to hide, but also to undertake for their different activities. People take on different identities. Again, these possibilities can be taken literally as well as figuratively: *'unlimited'.* Both geographically and in time, involving real-time and on a global scale. This fluidity requires a flexible way of maintaining order, investigation and the development of a new kind of intelligence.

Digitization is also causing a schism demographically - a generation gap between digital illiterates and "digitized" younger generation; new 'digital divide'. Older people cannot comprehend these developments anymore and make minimal use of the growing opportunities. The young generation is accustomed to these opportunities and expects to have information available, regardless and independent of whatever medium is available, time and / or location. In this context it is important to realize that the policemen are recruited from the same youth. Already, the young police officers have significantly fewer opportunities available at work than in their private home situation: *the new unreality@work!!*

Due to technology and the increased social individualism some other developments occur also. Looking at the development of technical computing networks it all started with the Wide Area Network (WAN), the Metropolitan Area Network (MAN) and mainframes. In the late seventies the first Local Area Networks (LAN) were taken into service and nowadays every company and even a great deal of households have their own Local Area Network connected to the internet. The next phase will be the Personal Area Network (PAN) in which the individual is surrounded with technology and creates their personal information sphere. The first PAN's arrived with sophisticated mobile phones and broadband Internet. With this an individual can take all the information, pictures, music and

connections with him; being truly mobile. To go full circle the next type of network would than be the global area network (GAN), built up from all kind of smaller networks and nodes. In fact the Internet equals the GAN.

Another example is the availability of information itself. Without broadcasting services (radio, television) only the governmental, scientific, religious bodies had specific information, which in general was not shared with the public. With broadcasting services being present information was shared increasingly, but a lot of information was tied up in 'closed' companies. Knowledge was power and therefore knowledge was not shared. Nowadays, the Internet provides an increasing level of global information to everybody and it provides an access to the collective intelligence[3] of the Global Information Network (GIN). Still the majority of large companies protect their strategic information, but the few that use the cloud as a strategic level of communication improve their business results.

A good example is the example of the US based gold mining company who organised a contest for new and unconventional ways of mining in order to get more gold out of the soil. The company put their strategic gold mining information on the Internet and asked for help. The winner of this contest would earn USD 500.000. Many people competed and a winner was congratulated soon after the start of the contest. But in all honesty, and that is the deeper meaning behind this story, the true winner was the company itself, because of the increase in the company's turnover exceeded the prize money many times.

The power of information shifts towards the public and the individual. In that way there is a similarity with the situation hundreds of years ago. People were in small tribes or travelling by themselves. The big difference now is that the individuals are connected through a network; that makes them stronger than ever before. There is also a threat that big companies like, Microsoft, Google or Facebook have so much power over individual data that they can easily rule the world. Already we see increasing government and commercial legal challenges particularly to Google.

The development in the energy market resembles a great similarity. In early days people themselves created energy by making fires and using the wind to power certain equipment. The energy market started to grow when stone coal, and later gas, oil, solar power, wind power and nuclear power, were used to provide energy. That era started with large centralized and government owned energy companies. The next development, in most of the European countries is the separation between the network part of the energy supply from the customer part. In fact it was a movement to break the power of market dominance. In

future, with the use of solar technology, every car will be its own solar power plant and the car is able to upload the stored energy to the household and to the network. So the network will not only provide the energy to your home, offices and factories, but is fuelled also by micro energy plants like cars, houses and so on. This is a shift from a decentralized energy model (pre industrial era) to centralized model (industrial era) and then to a network of collaborating nodes (information era).

Another example of the 'big' shift from a centralised 'command and control' mechanism towards a very decentralised 'communicate and collaborate' mechanism is seen in the automotive industry. Road management systems, which manage the traffic on the roads and try to predict and prevent traffic jams, are centralised. Intelligent cameras, road signalling systems, and predictive models are trying to inform the car driver of road usage and traffic jams ahead. It is a centralised system that informs road users.

Compare that view with a normal hierarchical organization, with a strategic, tactical and operational level of working and top-down steering. Compare it also with the television: other people decide on making programs and sending these shows, new flashes, entertainment, educational programs one-way to the viewer. In the near future the car will be an intelligent network node and provide information to the network in order to action events to happen. That will pave the way towards very intelligent services for improved safety, traffic management (floating car data, road billing), infotainment downloads, Internet access, diagnosis and repair and security. Road management will then change from a centralized to a de-centralized network model of small intelligent nodes. In fact cars themselves will manage traffic and predict traffic jams.

More emerging technologies are the creation of intelligent devices through artificial intelligence. The next generation modern wireless connectivity and 4G mobile networks will support the always-online ubiquitous mentality, where people have mobile broadband connections even faster than the current fixed cable connections. Translation functionality from text to speech and speech to text will make the communication between people and machines more effective. The developments in biometrics will enable in-depth unique individual identification methods and improve human-computer interaction. Solid-state drives will enable smaller, bigger (capacity) and cleaner (energy smart) data storage. 3D displays and screenless displays will develop the digital world even more to its physical equal and immersive virtual reality which is an artificial environment where the user feels just as immersed as they usually feel in consensus reality. Last but not least quantum mechanics, biomechanics, nanotechnology, micro machines and smart robots will fundamentally change our lives, the way people

work, social security, communications and collaboration. People and machines will be more than inter-dependent and we will become 'fused' in the sense of how they interact in the glocal socio-economy.

ALCOHOL AND DRUG USE

The acceptation on drinks and drugs usage changes severely. There is a tolerance to the use of alcohol and drugs. Despite the fact that the long-term effects become clear, it becomes more common to use cocaine at the weekend, one pill during a night out with friends and heavy drinking before going to a bar. The availability of particular drugs plays an important role in social security.

CARE FOR YOUTH

Although the majority of youngsters are trying to make the best out of live and stay out of trouble, problems and safety issues surrounding the increasing minority is growing. A few indicators for this are the increased demand for help with education, an increase of young people who exhibit criminal behaviour, increased drinking and drugs behaviour, the emergence of youth gangs and criminal behaviour increasingly among girls as well. One of the aspects of this 'development' clearly is the fact that society investigates more on the subject and creates more information. More information on the subject focuses society on a problem that seems to exist only now.

AGING AND IMBALANCE

Reports of worlds ageing of population[4] provides a description of global trends in population ageing and includes a series of indicators of the ageing process by development regions, major areas, regions and countries. The report shows that:

- Population ageing is unprecedented, without parallel in human history and the twenty-first century will witness even more rapid ageing than did the century just past.
- Population ageing is pervasive, a global phenomenon affecting every man, woman and child but countries are at very different stages of the process, and the pace of change differs greatly. Countries that started the process later will have less time to adjust.
- Population ageing is enduring: we will not return to the young populations that our ancestors knew.
- Population ageing has profound implications for many facets of human life. Nowadays there are many "rich" elderly, but in 2020 poverty amongst these elderly will be increased.

INTERNATIONALIZATION

Internationalization is a major influence on how the security of citizens and businesses can be maintained. The area of responsibility of the Netherlands has

international borders with neighbouring countries and at sea. The threats are "boundaryless": terrorism, globalization, massive increase in international traffic, organized crime and large-scale disasters are real threats. Internationalisation probably will increase mutual dependencies, which could easily lead to a domino effect of triggers of events. On the other hand the international community is strengthened as a network configuration and less sensitive to all kinds of imbalances. To deal with imbalances it requires ways of collaboration with partners in public safety, not only nationally but also increasingly internationally as well. It may seem to be a very pessimistic future for people. Considering the recent documentary: 'the age of stupid'[5], disorder may even happen. Fortunately people are Darwinists in their core and keen on continuing their lives and the lives of their children.

Information economy

The term information economy is used rather often to point out the difference between the industrial era and the information era. There is a strange contradiction between the terms 'Internet' and 'economy' though. The Internet is an almost unlimited source of data, applications and computing power, whilst 'economy' is, in the traditional sense, used to express scarcity and abundance. Because the demand always increases and shifts towards new products or better products, the need for almost unlimited resources applies here, but does humanity have unlimited (physical) resources available??

In the traditional science of economy the scarcity of a resource and the demand for that resource or product play an important role. High volumes of a certain kind of resources in combination with a low demand for the resource bring the price down and high demands for scarce resources bring the price up. But what is a resource? Does a resource exist? Normally the answer to that is 'yes', but looked from another perspective one could say that a resource is an invention of the human brain in combination with the use of technology. In this context technology is: "a new and modern way to do things you were used to do in a better and more efficient way".

We accept now that our domestic waste is a resource, but it wasn't a resource 30 years ago. At that time waste was just waste, now it is either reusable or transformed into bio-energy. Now we belief that the ground we are walking on is a resource, but long ago it wasn't. Ancestors would have laughed their socks of when people would have proposed to buy land without buffalo's. The buffalo's where their resource for food, the ground was no resource until somebody designed a new technology to farm the land and to create a new resource. So technology defines what a resource is. Technology defines also how much resource is available to use. For instance look at the oil or gas reserves.

Technology defined oil as being a resource, long ago oil was just a by-product; a form of pollution. Nowadays oil is the number one resource and traditional leaders warn that the oil is a scarce resource. If technology provides for a new engine that runs 50% more efficient, the need for oil decreases with 50% and it seems to be that the amount of oil doubled, which isn't technically true for obvious reasons. In that sense technology also defines how long people can have the benefits of the usage of that particularly resource.

But what controls the advance of technology? The answer to that question is that the speed of exchange of information controls the advance of technology. If a person would live alone for all his live, how many technological inventions would they have done? Would they have done more inventions if they got information for other people to perform a task better or quicker?? Probably yes, and if they had a whole community to work with the number of new technologies would probably be countless! In history we see also that new resources, again invented by humans applying technology, initiated a new era. For instance, inventing the resource 'stones' initiated the stone era (5300 BC), inventing the resource bronze initiated the bronze era (2100 BC), inventing the resource iron initiated the iron era (600 BC) and inventing the resource coal initiated the industrial era (late 18th century). In that way technology defines-resources, which build economic value, prosperity and wealth.

These theories worked for centuries and centuries; will this trend continue or change with the Internet as new technology and 'information' as new resource?? Will information be the 'new oil' that drives a new era and accumulates value, prosperity and wealth? The interesting part with this theory, applied on the Internet society, is that the Internet is built around the communication between people (social media) and that the speed of exchange of information is unlimited. An unlimited speed of exchange of information would mean unlimited technological opportunities and per definition unlimited resources. In the near future value, prosperity and wealth will come from information based business opportunities. The question for society is to balance this new resource in terms of justice, well-being and wisdom. The difference with modern Internet society is that the number of technology breakthroughs will be much higher than ever before. The past proved that technology would change over a lifetime. Nowadays technology changes several times in a person's life. For an individual it means that they must adapt quickly to new technologies or fall back. For businesses and governments it means that they must implement, nourish and stimulate the process of change and innovation because this will keep the organization going and improving.

Next policing; the paradigm shift

If one would describe the Dutch police[6] in the post war era it would start in the late 50th as a semi military organization servicing mainly the mayor, for an administrative task, and the public prosecutor, for juridical tasks. In the late 70th the police became a more society-oriented organization, in which people in the cities, suburbs, quarters and communities where the main focus for police work. In that way the police became an organization to protect and serve the citizens. A few decades later, early 21st century, the police developed itself as *co-creator of social security*. Not only the police was responsible for safety, but also local government and citizens themselves own that responsibility. Also in this area the shift from one big semi-military policing body in the late 50th towards a social security agenda owned by citizens connected with the government shows the same development as the described technological development from the wide area network towards the personal area network connected to the Internet; this is the paradigm shift.
Since a paradigm is nothing more than a fundamental set of rules and regulations by which people 'play the bigger game', it is absolutely necessary to redefine the rules in a transformational era. This in itself is not new, because each and every time paradigms are shifting and new principles apply. The world we are shifting to is characterised as being 'chaotic'; or at the least being highly complex where cause and effect are not easy to link before an event occurs. People will never understand it as we used to do and people or governments are never going to control it. Instead the society has to be responsive in every aspect of that society. So instead of being stable and controlled, people, businesses and governments need to develop their agility.

This paradigm shift towards an uncontrolled and agile environment however revealed itself in a few years; that's the challenge! The time to adapt is relatively short and that makes it difficult to change for the better. Individuals redefine the new principles of communication, interaction and collaboration quite quickly. Commercial organizations drive their developments by commercial goals and the pressure of boards and stock markets. Commercial companies will foresee these developments in an early stage and redefine the rules before losing competitive advantage. Governmental bodies, i.e. the police organization, work differently. They tend to be more reactive, because the pressure is not on the competitive edge, but on transparency, stability, legitimacy and work based on a legal framework.

The way the police treat information must be set and redefined on a strategic and administrative level. With the Internet being present and the availability of *information* on a global scale, the power shifts towards people that use and share information. The definition of the rules for an innovative police organi-

zation must therefore change. *Innovation* is about agility, flexibility and 'processes on the fly'. Innovation is key to any market and the way people, businesses and government adapt to the 'new world' and is the true meaning of survival of the fittest. Information and communication technology is a strong driver for innovation now and even more in the future. The police have to redefine the way Information and communication technology has been taken care of. Can the organization proceed on the current path, or does it need a complete turnaround with the face towards it citizens? Can the police serve better with more corporate functionality or with increased connectivity?

The game is not really to decide which is best, but to decide and follow through in all aspects. *Collaboration* rules must be redefined. Nowadays the police can hardly communicate freely with other governmental bodies, due to legislation and all kinds of boundaries. Why is that and what does the government in general has to change to be able to create a stronger co-operating organization and to tap into collective intelligence? Does the police need more 'partners in crime'? To tap into collective memory, government must redefine the meaning of *openness* and find a way to be agile, open and at the same time set a new standard for *integrity, security, transparency, trust* and *confidentiality*. If the police wants to keep their social legitimacy it's *evident* to set and redefine the meaning *connectedness* from shared societal values. As described, *decision-making power* shifts to the knowledgeable, information-sharing individuals and towards communities. With the police living in their unreal bubble and not being agile, how must strategic management set and redefine the rules of *self-organization* and *sustainability* to be able to 'protect and serve' in the new world.

To change the behaviour towards an open society is difficult to grasp. Why? Because the paradigm shift applies here too. The world in which the police organization would like to adapt to is quite different. Normally, in the previous era, it would be carefully planned; as it was the build of a railroad with agreed upon destinations predetermined stops and rigid schedules to minimize the risks taken. There was no room for flexibility or adaptability. Since the global changes are nothing like a stable process, the police needs a different approach in this dynamic environment. In fact, with hindsight, we can see the 'steady state' of the world is in fact one of constant change! This requires an organization to embrace uncertainty, dynamics demands from the business and to a certain level of chaos. It is possible because the infrastructure, i.e. the Internet, is already in place and constantly changing. This also needs a different mindset and is again a part of the redefinition of the so-called paradigm shift. The prevailing paradigm determines what you think is feasible, as well as what you think is the right way to execute change. In order to be

successful, the police organization needs to perform on the edge of chaos; semi-autonomous agents acting in accordance with simple rules towards a common goal.

Above-mentioned issues of defining the paradigm shift in detail taking consequences and changing for the better are often placed on the 'too hard' pile or 'the next generation pile'. Tackling these issues head-on has the benefit of not only orientating toward the *new connected reality*, but also shining a light on the root cause of long-standing issues where best practices are helping perpetuate the problems. More pressingly, people are beginning to solve issues for themselves. People are solving crimes where local justice agencies either cannot or will not help. This accentuates the new questions the police have to ask themselves.

---

[1] Referencing to a global event September 2009

[2] People live on the web, cybercitizens or persons actively involved in online communities. First introduced Michael Hauben,1992

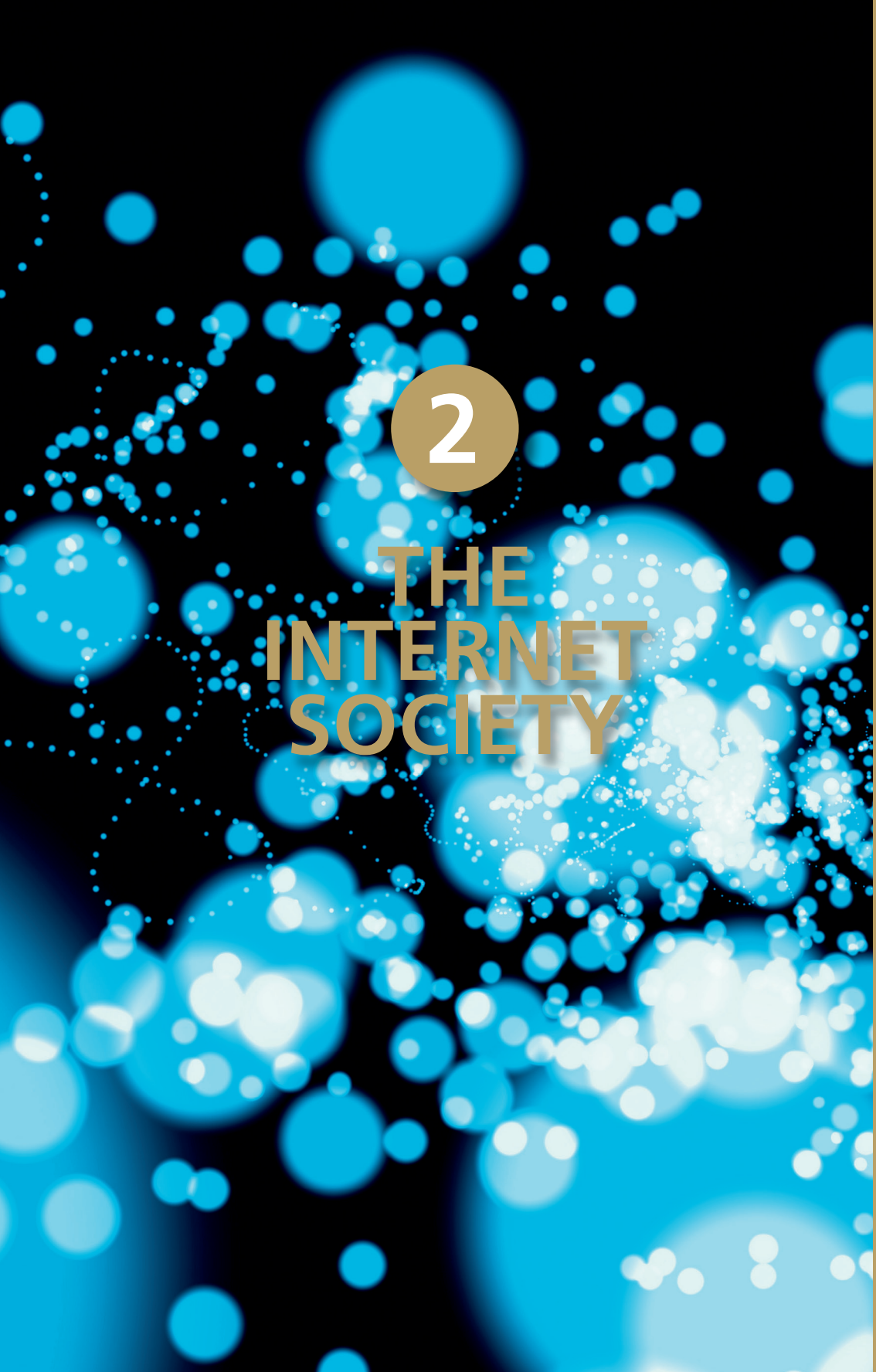
[3] The wisdom of the crowd, why the many are smarter than the few and how collective wisdom shapes business, economies, societies and nations, published in 2004. A book written by James Surowiecki about the aggregation of information in groups, resulting in decisions that, he argues, are often better than could have been made by any single member of the group.

[4] World Population Ageing: 1950-2050, department of economic and social affairs, United Nations New York, 2001

[5] The Age of Stupid is a 90-minute film about climate change, set in the future from movie director Franny Amstrong

[6] The Dutch police is an example here and can be translated to almost any west European country

[7] In Holland book 'Politie in verandering' was launched in 1977



2

THE INTERNET SOCIETY

Chapter 2

The internet society describes the new digital society in general and elaborates on the development of new crimes and the changes for the police organization. The Internet has already ‘happened’ to society and most of us realise that; the paradigm shift is a fact. Now society must learn to understand this shift and adapt the new rules accordingly. For the last decades, corporate and administrative leaders led their business based on their traditional knowledge and powers. Now information availability is phenomenal and it marks the Internet as the ultimate power distributor. ‘Living in a bubble’ wasn’t a problem for the police organization in 1999. Only 10 years later it became a serious challenge. The police organizations must redefine their business to be able to create a sustainable environment in which they can support a network oriented safety concept.

The Internet as we know it now pulls society towards the information society. Society is in the middle of the paradigm shift and it is beginning to understand the magnitude of this substantial change. This is obviously not the first paradigm shift people have lived in. The previous paradigm shift was the shift towards the industrial society started late 18th century; it changed where and how we live now. For instance, while the early stages of the Industrial Revolution gave birth to the modern metropolis - huge cities acting as economic and social centers, - the later stages of the Industrial Revolution, such as that involving the development of the internal combustion engine, gave rise to suburbs, highways, and dramatically increased personal mobility. Thus, that revolution completely overhauled both the geography of the industrial countries and the way social life was organized. Whole communities were destroyed and built as a direct result of these economic breakthroughs; often in just a matter of decades.

It is unclear what the overall effects of the Information Revolution would be in changing social relationships and geography. The creation of the information superhighway, for instance, could conceivably have effects on demographics as dramatic as— but very different in character from—those caused by the Industrial Revolution. For instance, with geographic location diminishing in importance to the information process, people may be free to live in remote locations; at the least, people may be less bound to certain locations, potentially leading to vastly new kinds of communities and other social organizations. The physical production process of goods still depends on the location, although, with professional logistical partners, a company can easily select the best location for its production process, based on profitability.
In terms of social relationships and relationships to the production process, the Information Revolution has indeed led to radical transformations. The mass-scale, centralized-factory paradigm of the Industrial Revolution featured a production process in which individual workers were relatively "de-skilled" compared to their predecessors, and had only to perform minute functions requiring little training and with little overall understanding of the production process as a whole. As a result, companies were able to produce at vastly accelerated rates while keeping costs down, leading to tremendous profits that, in booming times, afforded them the option of paying higher wages in order to quell labour unrest. On the one hand, this created an economic environment in which centralized, hierarchical managerial bureaucracies were essential to organize production and maintain control over the production process. The centralized factory created an atmosphere in which it was relatively easy for workers to organize themselves for greater remuneration for their labours.

In comparison, the Information Revolution presents something of a paradox. With computers, information technology, and high-tech communication systems

dominating the business environment, production can be scattered across diverse locations and coordinated at high speed with great precision. This allows businesses to concentrate their particular production facilities where they are optimally efficient, for example, where labour costs and regulatory red tape are minimal, leading to greater profit margins. Moreover, the movement towards computer controls creates a less egalitarian environment for wage-workers than the mass assembly-line model, since it creates a hierarchical advantage for those highly educated workers with technical skills. Decision-making could potentially be decentralized because of it and located at the various production facilities. At the same time, however, despite the geographical dispersion of production and the more nuanced worker relationships, information systems give top management greater direct control over the production process. By systematizing facilities via computers that provide reliable information across wide networks, top executives have a diminished need for middle-level managers, leading to the potential of downsizing and restructuring the features that characterized the 1980th and 1990th; whether that was successful or not.

Moreover, the geographical dispersal of production facilities and the enhanced means of computer controls overhauled the relationships between workers and the nature of work itself. In the information economy, work is much more flexible, favouring more fluid schedules and multitasking, in which workers are expected to perform several jobs more or less simultaneously and respond to immediate demands as they arise rather than coordinate their work solely by the clock. This radical restructuring of work in the late 20th and early 21st centuries had a profound impact on the role of organized labour in society. Flexible schedules and dispersed production facilities render the traditional models of labour organizing extremely difficult, and by the early 21st century no dominant model of labour organization had emerged to suit the information economy.

The transformation of work was potentially even more dramatic than that produced by the Industrial Revolution,in the information economy, nearly every profession was likely to undergo radical alteration as computer systems and the Internet infiltrate the farthest reaches of the economy. In the Industrial Revolution, many knowledge-based occupations, such as accounting, were relatively unaffected qualitatively by the sweeping changes produced by industrial development. The Information Revolution was unlikely to leave many layers of work untouched, as everyone from knowledge-intensive workers to manual labourers and government officials, would likely to see the routines swept aside in favour of more computer-intensive processes.

Industrial parts producers, for example, are accustomed to working an assembly line in more or less consistent fashion, building products destined for distribution

via long-established logistics partners. With information technology leading to supply chain management, just-in-time manufacturing, and mass customization, production processes were being retooled to facilitate greater flexibility in production scheduling, while distribution and transactions were increasingly channelled through handfuls of industry-specific Internet-based marketplaces.

As the Internet is the technological cause of the transition towards the information era. it would be worthwhile to elaborate on the Internet first and than to step towards the *social impact*, opportunities for policing and its information and communication technology function. The answer partly lies in understanding the 'largest human information construct' in history, i.e. the Internet, which is transforming society. Over the past 10 years the Web has led to a fundamental shift in how business, government and society uses and shares information. Understanding this shift, - from 'information technology' to 'information systems' , - is the key to delivering results in the global age: *'Providing the IT that fosters an effective, ubiquitous and responsive information system environment, centred around people and the information they need'*. People around the world use the Internet by clicking up to 100 billion times per day. By doing that mankind automatically teaches *'the machine'* with each click. Each and every click represents a little bit of information. Put together it creates intelligence, knowledge and understanding, which can than put together: trends, analytics and several insights. There is no way this global development can be seen as a pure technological development. It is huge and it will have consequences to society, as we know it now, even to people as we know them now. Human beings are part of this development and will adapt to the changes; *the Internet plus Humans equals the largest Socio-Technical system the world has ever seen.*

The Internet was invented and constructed early 1970th in the USA[1], is a global digital computer network that potentially connects virtually anybody to anything. Robert Kahn used the term Internet for the first time in 1974. It started for military purposes and soon found its way towards universities and businesses. A key success factor of the Internet is the fact that this construct doesn't belong to anybody; it's free to use. In the early nineties Tim Berners-Lee introduced the World Wide Web (www) and published the first Internet pages. Between 1994 and 2001 the commercial industries where using the Internet as an extension of their activities. The Internet was no more than a virtual display of the company's products or a digital information source. For example the Internet was used as a phone book, an encyclopaedia or a means to exchange information (e-mail). In fact the Internet was a virtual world at a distance and apart from the real world. This is what the public called Web 1.0 or the 'read-only Internet'. The Internet was a digital duplicate of the real world: producers stayed producers and consumers were consumers. The Internet was designed to be

robust and keep stable under (foreign nation state) attacks, but it has a couple of disadvantages as well. The existence of digital viruses, the lack of privacy and global privacy laws, new crimes, new identities and the fact that a data centre uses more energy than a normal industry would do, are a couple of those disadvantages.

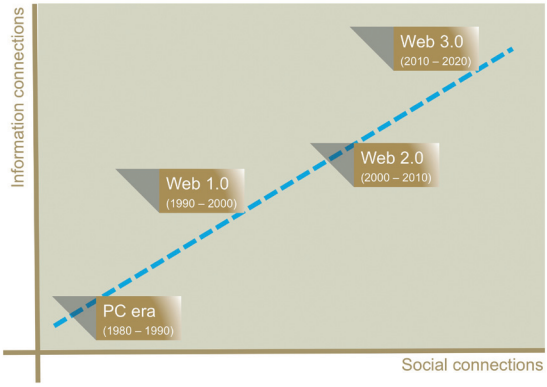
Due to broadband connectivity the use of the Internet exploded from 2001 onwards and created the global invisible infrastructure. In the next phase of the Internet, collaboration, sharing information and social media are key elements. The Internet has become communication central. This Internet era is called the 'Internet of people' or the 'social web'. People communicate with people and they collaborate through the Internet. The Internet becomes a global platform on which everybody can communicate, collaborate, share, create, build and maintain relationships. Consumers became more and more pro-active and could *produce* relevant 'user generated content'[2] at the same time they were consuming other content. People could easily build their own radio station and broadcast to those who like the music. People became information 'prosumers', professional users of information or producers and consumers at the same time. This point marks the paradigm shift towards the information era. Web 2.0 was born. All kinds of social media, professional networks, (micro) blogging networks, wiki's, collaborative tools, knowledge sharing networks and open sources take care of human demand for information. Information sources tend to become more and more multi-media where any type of information can be linked to any other type of media. Types of information sources are no longer linked together through a classification of a hierarchical set of attributes (taxonomy), but through a free set of tags (folksonomy). Data will be more and more semi structured or unstructured against a set of structured data elements in what we now call a typical database. An important aspect of the future Internet, Web x.0, is the concept of 'linked data', which refers to a method of identifying, showing and sharing unified resources. A unified resource can be a camera, a car or any other thing with an IP number.
Information sources will be mashed up in a way that meets people's needs. A mash up is a layered set of data sources tagged together onto one screen; multiple sources and one view. An example of a practical mash-up for policemen is Google maps combined with socio-economical information and the density of burglary incidents. A very practical tag is the geo-tag, because most of the things are interesting to people from a geographical point of vies. Again: people's communication first, than followed by technology or technocratic rules.

Technological advanced mash-ups are called 'augmented reality'. This is the area of computer research, which deals with the mash up between the real world and the virtual reality. Computer-generated data are blended into real footage

in real time. Based on GPS positioning, a live video stream and location based data it's possible to show specific points of interest on a mobile device. It would be possible to see 'houses for sale', 'restaurants' or 'the best deals in town', just by looking on your mobile. But it's also a more advance tool to see where criminals live, whether a truck with suspicious load finds itself in a certain radius or where a crime was committed; the virtual (digital) world projected on the real world. Advanced research includes the use of motion-tracking data, fiduciary markers recognition using machine vision, and the construction of controlled environments containing any number of sensors and actuators. There are benefits for police business in this, but it must be explored and tried out by the organization in piloted areas first.

The Web 2.0 era is also the end of the 'user'. As the term user connects well in the old world where a user uses a computer system or application to put information into a system and to get it out at an appropriate time. A user is more likely to be a 'requester' than a pro-active actor. So, pre-web, people are serving the machine and computers are record keeping instances connected to a smaller or larger network. But the world is a global information system and people are using this global information system. They build knowledge to the system in a natural way, most of the time without knowing that. For instance if you look at Google Insight, Google can predict events (e.g. flue epidemic) quicker and more accurate than a branch could do, just by analysing the global click behaviour on the Internet. This fact alone has obviously consequences for 'old users' in terms of 'old behaviour', but has also consequences for managerial behaviour. As a participant in the information sphere, to achieve a goal, it's the combination of the information in ones head and the information on the Internet that counts.

Is it done yet?? Is web 2.0 the end of the line, certainly not! Web 3.0 is called the semantic web or the intelligent, ubiquitous – or pervasive web. In fact the Internet as we know it now breaks out of our screens and is available anywhere, anytime and on any device.



"I have a dream for the Web become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The 'intelligent agents' people have touted for ages will finally materialize."

By 2029, sufficient computation to simulate the entire human brain, which is estimated at about 10^{16} (10 million billion) calculations per second (cps), will cost about a dollar. By that time, intelligent machines will combine the subtle skills that humans now excel in (essentially our powers of pattern recognition) with ways in which machines are already superior, such as remembering trillions of facts accurately, searching quickly through vast databases, and downloading skills and knowledge.
Tim Berners-Lee

But this will not be an alien invasion of intelligent machines. It will be an expression of our own civilization, as we have always used our technology to extend our physical and mental reach. We will merge with this technology by sending intelligent nanobots (blood-cell-sized computerized robots) into our brains through the capillaries to intimately interact with our biological neurons. If this scenario sounds very futuristic, it's good to know that blood-cell-sized devices exist and execute that are performing sophisticated therapeutic functions in animals, such as curing Type I diabetes and identifying and destroying cancer cells.

The next web is also called the 'Internet of things', where people become connected to things and things connect to things. Photo frame's connected to the Internet can upload photo's according to a profile. Cars can communicate to garages and garages communicate automatically with suppliers of spare parts. The world is connected in the information sphere, were software has become a service instead of a software package and is delivered through network computing. The use of open sources is a commodity and people have second or more identities. People and machines are identifiable by a specific, but constantly changing, IP number and their profile. Based on the profile, things actions take place. But what is meant by the word 'semantic'? Semantics are the meaning of a word or sentence. A semantic web means that the Internet cannot only see the syntax of a sentence, but can also understand the meaning of it. The name 'Paris Hilton' will normally refer to the person Paris Hilton and not to a 'Hilton hotel in Paris'. In this case the syntax is the same, but the semantics differ. If you analyse the sentence: *'Mieke loves Mike'*, than that's clear to he computer. If you change the word 'love' in a symbol, like:♥, than the syntax changes, but the semantics, or meaning, remains the same.

Today's computers can't handle the difference between syntax and semantics. It is the same as when people do a search request on Google. Google replies with a number of pages, but doesn't really understand what the question was. In communication between people, the difference between syntax and semantics is very important. In fact it is one of the few significant differences between humans and computers.

The current Internet is a document related Internet. With search requests you will get documents back. The documents are filled with all kinds of entities like: persons, places, events, sports, locations etc. Web 3.0 gives a particular meaning to entities and relationship between entities. Meaning is not a clear single attribute of an entity, the meaning of something has to do with individual perception and could change over time and in different situations, the semantic web will get as close as possible against the profile of the requestor. In the example of 'Paris Hilton', for you as a participant it would be nice to have that recognised as a hotel and to get additional data on the reservation, the flight, car rentals, restaurants and even other things that connect your profile to your search request 'Paris Hilton'. The value for police business of this type of development is tremendous, because police business is all about pieces of data, links between data and the meaning of data in their context. It's almost an obligation for the police organization to step into this new world of supportive tools, to put it modestly. It is obvious that Web 3.0 leads to a greater availability of meaningful information and therefore tends to contribute more to the subject of information overload. Though, people need information exactly tailored to an individual. In addition to HTML and XML the industry works on APML (Attention Profile Markup Language), which envisages to do exactly so. The Internet will be personalized as well in a way that an individual can construct his specific needs on the Internet. Although this may seem to be possible from a technological point of view, the intellectual skills will create a real hurdle.

In a Web 3.0 driven society the meaning of a second or third identity grows. For instance if the number of camera's grow in public area and camera views are linked to real people, based on facial recognition and virtual profiles, than one can see the tremendous change of an information driven society. Web 3.0 means that everything and everyone becoming connected, people and machines becoming fused and finally it will support and drive a transformation from a product-based to service-based economy.

> The web changed my life. I can't live without Wikipedia or Google. But ultimately, I'm disappointed. Almost every day, the web lets me down. What do web makers and participants do for a living? What do we get paid to do that makes it worth giving us a web browser? Me, I make connections, I am a connector. I take disparate ideas and connect them in (hopefully) useful ways. Others do it with people, or cash instead of ideas. *But we're all connectors.*

The opportunities of the semantic web are limitless. But that's not Web 4.0. And it's entirely possible that Web 4.0 will get here before the semantic web even though Web 3.0 makes it work a lot better. Obviously it starts with ubiquity, identity and connection. Ubiquity is needed to build Web 4.0, because it is about activity, not just data, and most human activity takes place offline. Identity is needed to build Web 4.0, because the deliverable is based on who you are, what you do and what you need. Connection is needed to build Web 4.0, because you're nothing without the rest of your environment; the people.

Web 4.0 is about making connections, about serendipity and about the *network* taking initiative. Web 4.0 implies that machine intelligence has reached a point that the Internet becomes the planetary computer, a massive web of highly intelligent agents.

A scenario with a twist of provocation

I'm typing an email to someone, and we're brainstorming about doing a business development deal with Apple. A little window pops up and lets me know that David over in our Tucscon office is already having a similar conversation with Apple and perhaps we should coordinate.I'm booked on a flight from Toledo to Seattle. It's cancelled. My phone knows that I'm on the flight, knows that it's cancelled and knows what flights I should consider instead. It uses semantic data but it also has permission to interrupt me and tell me about it. Much more important, it knows what my colleagues are doing in response to this event and tells me. 'Follow me' gets a lot easier. Google watches what I search. It watches what other people like me search. Every day, it shows me things I ought to be searching for that I'm not. And it introduces me to people who are searching for what I'm searching for. As a project manager, my computer knows my flow chart and dependencies for what we're working on. And so does the computer of every person on the project, inside my team and out. As soon as something goes wrong (or right) the entire chart updates. I'm late for a dinner. My GPS phone knows this (because it has my calendar, my location, and the traffic status). So, it tells me, and then it alerts the people who are waiting for me.

At this point in time even Web 0.0 is not understood by a vast majority of corporate and administrative leaders, management and employees in commercial and non-commercial companies, let alone the above-mentioned developments. In the middle of the transformation era, another technological development is happening and will support Web 4.0 onwards. We are at an early stage of this transformation – the convergence of nanotechnology, biotechnology and information technology is one example of an area in which there is likely to be rapid – and potentially disruptive – change in the next decade.

The 'big switch'[3] is fuelled by the development and availability of new technology and information. The big switch is a fundamental change in de nature of computing. Society is going from a time where computing is hosted, executed and used in a (semi) local situation to a time where computing is delivered over the Internet. In similarity it is the shift in the electric power over the years. A long time ago every household generated their own power to run electrical machines; local windmills are a good example of that. As soon as people got the network every electrical device could be plugged into the network via a wall plug. In near future everything that can use and produce electricity will come with its own power supply and will deliver its power surplus to the network.

The Internet will be a global computing platform[4] instead of an information platform. In due time people, co-workers, working groups and professionals will deliver their information or applications to the web. Where the web first was a source of information and an add-on to the business technology platform, it now becomes a computing platform again where people, businesses and governments find their information, computing power, applications and collaboration. A few major developments can be distinguished whilst the Internet is evolving towards a computing platform delivering a varied set of communication tools.

EVERYONE AND EVERYTHING IS BEING CONNECTED.
At one end of this trends it means that everything and everyone will get a connector or IP number. At the other end it means that if a person of a thing is connected to the internet it is connected to all other machines and people; globally. It's also related to the subject of the Internet of things, which will be a "non deterministic and fully open cyberspace" in which autonomous and intelligententities or virtual objects will act in full interoperability and will be able to auto-organize themselves depending on the context, circumstances or environments.

PEOPLE AND MACHINES ARE BECOMING FUSED.
Rarely people leave home without their mobile phones. And if so it is likely that people go back because of the 'empty' feeling of not being connected and therefore not being able to talk to communities, to get messages, to search on the internet and so on.

SHIFT FROM PRODUCT BASED COMPUTING TO SERVICE BASED COMPUTING.
The best example to explain this trend is e-mail. In the early days e-mail functionality was developed within a company. Later Microsoft developed outlook and exchange and people were able to send and receive mail through

an e-mail client and a hardware backend. Nowadays hotmail and other Internet services provide the same functionality, but without the trouble of licences, servers and local infrastructure. This type of 'soft-ware' is captured by the term "every-ware".

SHIFT FROM ORGANIZATION ORIENTED TOWARDS PEOPLE ORIENTED.
In typical hierarchical organizations the organization is the leading entity with a command and control structure, a board of directors and business processes to follow. Due to the 'big shift' this will change in horizontal structures or communities, where cross-business or cross-border communication and people are the fundamental changes. It is predictable that stream of money and the direction of power will follow these horizontal communities. The technological changes do not only fully change the way people work, they transform the nature of their social interactions. It changes the way an individual contributes to the global information - or global intelligence system. The Internet, mobile communications and social networking have a transformational impact on communities – building new, virtual ones and giving existing ones the chance to communicate in new ways. This needs to be seen in the context of globalisation of the economy, increasing movement across borders and the ability to share information rapidly and at low cost. A number of present businesses and governments issues are surfacing which require fresh perspectives, and the specific adoption of such new techniques, to address; again it elaborates on redefining key principles.

'Netizens'[5] are forcing governments to change track by analysis of their actions and sharing openly their perspectives of what's going on. If the assumption "knowledge equals power" is correct, the business and government collectors, processors, producers and distributors of knowledge – organizations as we know them – had better get to grips fast with new balancing of power with the individual. The real pressing question for organizations today is: *'Which parts of the current business model are susceptible to people 'doing it for themselves'?* What are the risks? What are the opportunities?

Anyone, at home, at work, can share information with anyone else. Inexorably, and globally, the shift is in moving from information consumers to information prosumers. This shift will not take place on a specific moment for all people, but will reveal itself gradually. A small portion of users will add valuable content, whereas the majority will only use available information. The shift is in moving from citizens to *netizens.* The *netizens* are people living on the web, communicating and collaborating through the web, participating in communities and working on future businesses. The web for citizens of the future is not an add-on, but the fundament of their lives; *netizens* live on the web. Laptops,

desktops, applications, information sources are all connected to the web. New forms of information security need to be implemented, because it cannot and will not be 100% open. It is connected, but no one will agree on having the more privacy related data free on the web.
The Global Area Network (GAN) is similar to all previous forms of networks, but is global and connects everything and everyone. It's equal to the Internet or the 'net.work'. People, applications, data sources, devices, business and governments all have their unique IP address and can communicate with anybody. The transition will take place from the IT landscape we know now towards cloud services, application services, social networks, geo-mashups, multi media devices and so on.

The rise of the Internet and technology

In this paragraph the fact that current information and communication technology function merely is "a record keeping" function against the lowest costs and the potential danger of that will be established. We also know that any business, in particularly government and policing, cannot maintain legitimacy without a incremental and continuous innovations and intelligence. Both, intelligence and innovation are fully dependent on the information and communication technology function of the police. The information and communication technology function is not only an enabler, but a very strong driver to create a sustainable business. The other conclusion is that the Internet is a 2 billion people computing platform and definitely version 2 of corporate information and communication technology. In future businesses don't need a corporate information and communication technology function with servers, interfaces, applications and firewalls; the Internet will provide it all. Business as usual is history.

The 1st and oldest form of society is that of "hunter-gatherers". Hunters live in small groups and are primarily engaged in the survival and the search of food. The innovation of hunter-gatherers is focussed on the creation of the fist weapons to hunt better. Centuries later they discovered that animals can be made tame and crops can be grown.

The hunter-gatherer learned to build settlements, making the 2nd form of society possible: *the agrarian society.* The production of food has been successful and people gathered in larger groups or villages. It was not productive that everyone dealt with the growing food emergency. Some people started to make clothes or tools and weapons. These goods were than exchanged for food. Then the industrial society arises in the 18th century by a number of technological discoveries. Machines are gradually replacing people, which lead to unemployment in society. The work moves from home to an office or a factory. The

computer makes its way into society. With the rise of white-collar workers the knowledge economy was born. The trend is that information-centricity will lead to further democratization and decentralization of organizations globally and that non-state horizontal powers will arise.

Douglas Adam's famously described *technology* as 'stuff that doesn't quite work yet!'. Yet technology is starting to work in the cloud. What's the future for our information and communication technology functions when information and communication technology is out there that actually works? Starting with that fundamental thought elaborate on the thought that with one billion iStore app downloads in one year, people aren't just solving life's little problems one app at a time, they are solving business problems too. Which parts of our policing operations today are susceptible to the new generation of IT? What are the advantages and issues?

The problem though with the current corporate information and communication technology function is that, quite naturally, is reflects, or mirrors, the corporate organization and processes. It reinforces information boundaries and flows, because these were designed in the previous era. In that way it doesn't support the redefinition of the principles of the information era. A few characteristics are that current information and communication technology functions connect well internally only and the security is based on an infrastructure or application level. Most of the time there is a lot of legacy, which cost a tremendous amount of effort and money to maintain, let alone to further develop or innovate. The legacy contains a lot of inherent knowledge from the business processes and is often not well documented. There is no free connectivity to the outside world and therefore no support for a modern form of communication. Information and communication technology functions are text driven and the so-called multi media sources cannot be used. To decrease costs employees are given a limited storage and mail capacity and different applications work hardly together.

Normally technology takes the blame for not performing; the opposite is true though. Technology does offer opportunities to create 'new' and added value to business innovations, but the management doesn't want to. This means that the police organization has to swap with information and communication technology 180 degrees around: from internal to external, from asset management to information management and collaboration, from closed to open. Technology has increasingly freed individuals within the organization and therefore the organization itself. Individuals in their private lives use technology to their horizon, meet new people, gain access to a very large reservoir of information and dynamic partnerships in order to make the best profit to be achieved. The organization gets the feeling of freedom when she is free to link

into the outside world, to tap into collective intelligence and to interact and unlock the collective memory. This definitely requires a flexible design process, (near) real-time access to data sources and a redesign of the fundamental principles for generating, collecting, analysing, using and sharing information of governmental bodies.

To take the information and communication technology function from the current level to the next level it needs to adopt some new principles. Information and communication technology is *people and communication oriented* and driven by the *Internet.* Through a combination of technologies the global user may establish or participate in partnerships, share information and acquire new knowledge. Users can personalize their needs completely. By applying personalized portal technology with devices that can display information, may transact, portable and everywhere connected to the Internet, new applications are used. Information and communication technology must support *unlimited collaboration* in a broad definition. Not only read, decide, buy and checkout is important, but finding new partnerships, interaction with other social networks and connect with customers, suppliers and competition, 7x24 on a global scale, is key. Other business models are emerging and other forms of acquiring knowledge (i.e. Wikinomics). Information and communication technology must support *agility and flexibility.* The speed of developments will also have an effect on the necessary agility and flexibility of organizations, including governmental bodies. The constant changes in the environment necessitate rapid adaptation of organizations. Business processes are dynamically arranged by the people (staff, citizens, consumers) undertaking the actions they wish to in order to achieve their goals. The underlying information systems must therefore consist of a dense network of configurable Internet services. Information and communication technology is *information centered,* which means that the business process is no longer the starting point of discussion, but the way people interact and communicate. A business process is nothing more than a representation of the way people have to work within the 4 walls. It doesn't explore the intelligence of people and it's doesn't use the available intelligence outside the 4 walls. Intelligent organizations are organizations that know how to handle available information (internally and externally) and use that to achieve strategic goals. This is done by constantly gathering, analyzing (analysis, reporting, risk assessments, visualizations) and integrate that into the primary decision processes. The constant enrichment of information from the outside world becomes a necessity. Standard services are packaged as standard software packages and applied "on demand" (software as a service) on and over the Internet (cloud computing). An example is Salesforce.com, which offers functionality for sales organizations through the Internet. So a two times advantage. First, because the functionality does not need to be devised and

the software no longer needs to be hosted within a corporate data centre. If the information and communication technology function is based on the Internet it can use the tremendous capacity of the wide spread *global broadband optic fibre network.* It provides an experience of "information and communication technology out of the wall ', like gas, water and light. In future there is no need for data centres as we know it today. The key question tough management has to put forward is: "what supports our business outcome more? More corporate information and communication technology functionality or more connectiveness?" *Open standards,* REST[5] architecture and to some degree service orientation are the three developments that underpin the previous ones. Since organizations are increasingly dependent on information, the need for "borderless" communication is evident. Open standards are of utmost importance when it comes to cooperation.

Many employees have more access to data and functionality from their home computer than they have from their company. That sounds familiar, but remains very strange. Billions of dollars are being spend on the innovation and maintenance of corporate information and communication technology and a single Macbook will out challenge it in the ability to access information quickly. This is called the *'black and white wire' – dilemma* and shouldn't companies have a structural white wire strategy? The black wire connects the employee to the corporate network, which is connected to corporate applications and the Internet, but only through a heavily secured firewall. The white wire is a standard consumer connection to the Internet. The black wire constrains the information and services an employee has access too. The white wire doesn't; it seems to be faster too!! Valid questions can be asked: 'why does the employee still has a black wire?', 'why would I implement my own corporate IT services?', 'why wouldn't I take them from the Internet?'. These are quite simple, yet deep questions. Consider corporately owned networks, PCs, applications, databases and data centres. And then consider the point of all of these things – to support business outcomes! But does this really work?? Nowadays we already know that between 60% and 80% of the usable data is outside the company's perimeters, i.e. an open information strategy with the Internet as fundamental basis. Given business outcomes depend more than ever on the connectiveness of an organization with the world via the Internet, there is a logic to using services on the Internet because by definition these have a global reach and their providers have often figured out in an IT sense at least how to secure information in the outside world. They are 'white wire' by default.

Using REST architecture, data, web services and applications from the web, also means using data from the web next to corporate data sources. Combining inside with outside is a big step for strategic management in general and information

and communication technology management in particularly. The latter is used to a fairly closed environment for record keeping purposes. Past decades the information and communication technology management has fought for more security and in a blink of an eye the world changed from 'closed and hostile' to 'open and sharing'. Many social network and micro blogs like Twitter are a good example of this phenomenon. It doesn't mean that the world isn't hostile anymore, but it means that the principle of sharing becomes a normal habit.

Corporate technology will be overtaken by *consumer technology* in its ability to access information. Corporate technology is driven by efficiency and a 'record keeping' culture. Consumer technology is driven by communications between people. This change boils down to the definition of the acronym: ICT, which stands for Information and Communication Technology.
By 'information' the branch means, keeping the records with highest integrity and security against lowest costs. 'Communication' means the technology necessary to support communication between people. In current organizations it often means peer-to-peer or one-to-many communications. It can be supported with a phone, e-mail or mobile SMS. These technologies work perfectly in the current setting. But the landscape changed. Our children don't know how to use e-mail or find it a modern way to write a letter, instead they use chat functionality (instant rewarding). Next generations will extend their communication repertoire by using many-to-many communications, like MSN and most of the communities and social networks.

The 21st century is characterized by a huge leap forward in information technology. Especially the impact of digitization on all sections of society is of paramount importance. The playing field is a global web-enabled platform where individuals, groups, businesses, institutions, science and government around the world continuously interconnect and work together, independent of the traditional barriers of corporate structures, time, country, distance, geography and, probably soon even language

Whether and how companies, profit or non-profit, benefit from this new development has to do with the emerging new vision and strategy of the organization concerned. The new business strategy is focused on horizontal communication, about outsourcing of non-core activities and with that setting up new forms of collaboration to be able to provide the best product. Furthermore organizations need to create a strategy to elaborate on the new and unique position in the information value chain and necessary skills and people management. The "command and control" structure is replaced by a "connect and collaborate" structure. The opportunities of the information herein are both the driving force: business strategy and information strategy

are coming closer together and the knowledge worker will be professionalised. Vertical hierarchical oriented organizations will be replaced by horizontal collaborative communities, mobility and movements will increase, people together will add value to the information sphere each and every time they use the internet and that individuals have the information and therefore they have increased power. This is one of the shifting principles of an information era that will change the business of policing.

A major dilemma now is that the current corporate and administrative management who are standing with their legs in the industrial society and their heads into the information era. The old patterns and existing solutions still dominate in the new context. A good example is the following.

> A mayor of a medium size city was challenged by a students strike fall 2007. He reacted as he would normally do and called his department to form a crises team and to setup the first meeting to see what is going on. His 15-year-old daughter overheard the call and wanted to contribute to the problem of her father. She looked on the Internet and foraged off the social networks. After 15 minutes his daughter knew exactly how the students would progress in this strike: whom the leader was, where the playground would be and what the next step would be. Traditional policy advisers were still in the process of organizing the first crises meeting.

Cloud computing

Businesses and their information and communication technology function grow from record keeping companies to a global computing platform, servicing a better information and communication technology experience than the current information and communication technology department does. The Internet causes this trend to develop due to global connectivity and also gives an answer to the solution of the massive change: *'cloud computing'.* There are many definitions of cloud computing, and therefore none. Cloud computing refers to computing resources designed to be available to anyone over the Internet. Contrast with the majority of IT in use today by corporate bodies, where the IT is owned and managed by the company itself. It's the same difference as ever corporate providing their own staff restaurant or your staff going outside to buy a sandwich and have lunch. The result is the same but the operational principles are quite different. Cloud computing is a simple concept, but with quite profound opportunities and threats when applied to information and the supporting IT.

Current IT environments contain large data centers and a number of services and an operating system and some kind of database on top of that. The

application stack is usually a combination of (old) legacy, different data models, a number of modern applications or user-interfaces, a large number of one-to-one interfaces to connect several applications to another, multi platform, language and programming standards. End-users use these applications on desktops, laptops or mobile devices. In most cases the end-user experience is multi logon, multi user-interface, no open external-in communication, very restraining security policies and hardly any valuable interconnection between the applications or data sources. To change this environment is time consuming, money spending and takes a lot of resources to do so. The cloud could potentionally change that over time and people will have to overcome faults and failures.

Cloud computing relates to the process of innovation, commoditisation and externalisation. Innovation is a process of finding new ways with or without existing or new technology to do the same thing or new things better, safer or cheaper. An innovation taken into mass production and use becomes a commodity. For instance the fact that people had access to the Internet was an innovation years ago and was used by the early adoptors; it was special and very few people used the access. Nowadays there are so many people using the Internet, that is has become a commodity. In new homes the buyer find optic fiber connections next to gas and electricity. Commodities can be outsourced of externalised to companies who are able to make, market, price, service and distributed the product. The difference between outsourcing and externalising is the level of relationship a company has with its outsourcing or externalisation partner. Usually the relationship with an outsource partner is closer and there is a service level agreement between partners. With externalised services are offered on a usage base, whenever and wherever the partner needs the service. Think of outsourcing as asking someone else to run your staff canteen; and externalisation as asking your staff to get a sandwich from the high street at lunchtime. This process is obviously applicable on all kinds of IT functions. From a technological point of view externalisation means that specific IT functions are completely moved out of the organization, even without closing a service level agreement with the provider. An example of that process is the email function. If you look at the data in exchange, the bulk of it is duplicated attachment. If companies provide their employees with access to an externalized unstructured storage capability ('content management in the cloud') such as that offered by Google docs, then email will contain URLs rather than documents and storage becomes much more efficient. As such the email function is no longer an IT function, but a service in the cloud. Since the Internet is a 2 billion people-computing platform, this is an interesting topic to elaborate a little bit more.

There are many definitions of cloud computing and therefore none. Cloud computing is about a transition or transformation and a consequence of many

factors. It is the same as the rise of the industrial revolution where technology, the attitude of people, new business concepts and the suitability of new concepts in time created the spark for the industrial revolution. Many innovations from that time transformed towards a commodity. Electricity is one good example. It started with an innovation back in 1820th and commoditised to a national grid in the 1930th. This process is called *'commoditisation'* and business competition between manufactures and providers drive this process. If one competitor creates a competitive edge, the others will follow soon afraid of falling behind.

Taking a big step forward in time, certain IT innovations are indeed suitable to transform into a service as well. The technology to do so is available for a long time. The concept of using this for business purposes is there also and the time is suitable. The only thing this process needs is a positive business attitude towards cloud computing. Nicolas Garr speaks about the evolution of business technology and explains that there is a diminishing strategic value in common IT as it becomes ubiquitous. And that causes the shift to an externalised IT function; disruptive for corporate IT! If a government of company decides, for any reason, not to evolve and adapt to this change, the gap between available (cloud) IT and own resources becomes bigger over time. Having a corporate IT function, as we have now, becomes then a *disadvantage* (functionality, time-to-market, financially) for any business.

Fundamental business advantages of cloud computing are the speed and time-to-market of new functionality for end users. Corporate IT can free up time from regular IT activities and retrieve that functionality from the cloud. With the 'free' time the corporate IT organization can build on corporate specific problems and solutions and close the gap between business and IT. Finally cloud computing can lower the cost by leveraging internal use of infra-structure more cost effective and using the public cloud and leveraging on the application stack of others and on the economies of scale of a large utility environment. In time cloud computing will gain market share and corporate IT will grow into more specific types of functionality, dealing only with specific vertical or company related solutions. Using the Internet as a computing platform will certainly introduce 'security' as a high priority discussion. Security issues and issues of misusing the power over data centers are not solved yet but very important for the success of cloud computing. The opportunities for the police are numerous and therefore it is highly recommended, almost obligatory, that strategic police management and political administrations must change the leading principles for information technology.

Cloud computing will be big, both in and outside of the governmental body. Being aware of the challenges will help business strategists. Here are 10 reasons governments and police forces[7] aren't ready to trust the cloud fully

now; but will in future!!

- It's not secure. Police forces have to maintain strict watch on their data at all times, either because they're regulated by laws such or because they're super paranoid, which means sending that data outside company firewalls isn't going to happen.

- It can't be logged. Tied closely to fears of security are fears that putting certain data in the cloud makes it hard to log for compliance purposes. While there are currently some technical ways around this, and undoubtedly.

- It's not platform agnostic. Most clouds force participants to rely on a single platform or host only one type of product. If you need to support multiple platforms, as most enterprises do, then you're looking at multiple clouds. That can be a nightmare to manage.

- Reliability is still an issue. Even inside an enterprise, data centers or servers go down, but generally the communication around such outages is better and in many cases, fail-over options exist. How does it work when critical servers go down in the cloud? Who is to call to restore quickly. This issue will be solved, but for now it is more comforting to have a company-paid IT guy on which to rely.

- Portability isn't seamless. As all-encompassing as it may seem, the so-called "cloud" is in fact made up of several clouds, and getting your data from one to another isn't that easy. This ties to platform issues, which can leave data in a format that few or no other cloud accepts, and also reflects the band width costs associated with moving data from one cloud to another.

- It's not environmentally sustainable. The computers are still sucking down megawatts of power at an ever-increasing rate, and not all clouds are built to the best energy-efficiency standards. The energy problem is still there but less visible.

- Cloud computing still has to exist on physical servers. As nebulous as cloud computing seems, the data still resides on servers around the world, and the physical location of those servers is important under many nation's laws.

- The need for speed still reigns at some firms. Putting data in the cloud means accepting the latency inherent in transmitting data across the country

and the wait as corporate users ping the cloud and wait for a response. Ways around this problem exist with offline syncing.

- Large companies already have an internal cloud. Many big firms have internal 'data shops' that act as a cloud to the multiple divisions under the corporate umbrella. These internal shops have the benefit of being within company firewalls.

- Bureaucracy will cause the transition to take a long, long time. Police forces and governments are very conservative. Transitions in core computing and data storage can take years to implement.

These issues will be solved in near future. parallel to solving these issues the organisation must prepare for the strategy to use cloud computing for their business.

---

[1] Tim Berners Lee, 1969
[2] User generated content is divers and multi media. From documents to internet sites, photo's, video's and music
[3] Paradigm shift from the industrial age towards the age of information
[4] A platform where people can use computing power as well as store and retrieve multi media dataa
[5] Netizens are people living and working on the Internet
[6] REST = REpresentational State Transfer. REST-style architectures consist of clients and servers. Clients initiate requests to servers; servers process requests and return appropriate responses. Requests and responses are built around the transfer of "representations" of "resources". (source: Wikipedia)
[7] Source: www.gigacom.com

3

THE INTELLIGENCE FLIP

Chapter 3

In general data quality in police organizations is poor, information processes are isolated, systems and functionality are not designed for building an intelligent organization and laws prohibit intergovernmental collaboration. The global trend is the availability of information anywhere and anytime on any device possible. From ancient history police depends on information to turn into beneficial intelligence and knowledge. What happens to the intelligence function in the global information era? In what way must the organizing principles be reset to keep an effective policing strategy? Can the police take the risk of having no strategic intelligence at all and how does this challenge the current models of 'unreality'. Senior management must make decisions about tomorrow, today!

Looking at the timetable at the right it is hard to imaging that in such a short period of time, humans have created such an overload of information[1]. This refers to the difficulty an individual can have making decisions caused by the presence of too much information. An individual or corporate body can no longer make the reasonably correct assessments on which rational behaviour is dependent. As the world moves into a new era of globalization, an increasing number of people are connecting to the Internet to conduct their own research and are given the ability to produce as well as consume the data. Information overload inherits the risk of unknown validity of information and even deliberate misinformation. As indicated before: police legitimacy depends on validity of information and making trustworthy quick assessments and decisions. Information is a strategic weapon for policing. Policing has always been about: information, intelligence, evidence, procedures, and criminal records. The growth of new technologies and the possibility of creating, managing and analysing new sources of information i.e. DNA, streaming video, digital pictures and so on, will become increasingly important.

Imagine what all the communications in the world today might look like if one would put it together. All the conversations, notes, letters, records,

Timetable

3500 BC to 2900 BC
The Phoenicians develop an alphabet.

1400 BC
Oldest record of writing in China on bones.

1270 BC
The first encyclopaedia is written in Syria.

900 BC
The very first postal service for government use in China.

14
Romans establish postal services.

100
First bound books

305
First wooden printing presses invented in China - symbols carved on a wooden block.

1560
Camera Obscura invented - primitive image making.

1650
First daily newspaper - Leipzig.

1714
Englishmen, Henry Mill receives the first patent for a typewriter.

1793
Claude Chappe invents the first long-distance semaphore (visual or optical) telegraph line.

accounts, documents, books, TV programmes, films, clips, recordings, pictures, music, emails, blog posts, tweets. If only the amount of information was taken from the internet and translated to 'books', one would see over few thousand stacks of books from the earth to the sun. Add all the information each of us observes as we're walking around which isn't consciously communicated – people going about their business, an accident, an argument. That would be a staggering amount of information. Not all communication from all of time is available to all of course. People in earshot can only hear the conversation you're having. The body language of a person is can only be seen by people in line of sight. Smoke signals from millennia ago are, of course, now unobservable.

The global tendency to economic instability caused by multi polarity, the scarcity of natural resources and the exponential growth of information space were pointed out before. These global developments will influence public safety and it is therefore important to understand the major and minor changes and to see new opportunities for policing.

In fact the current developments of the Internet indicate that information space almost 'explodes'. An unknown growth of Exabyte's of easily accessible information overloads people, government and commerce.

1814
Joseph Nicéphore Niépce achieves the first photographic image.

1821
Charles Wheatstone reproduces sound in a primitive sound box - the first microphone.

1831
Joseph Henry invents the first electric telegraph.

1835
Samuel Morse invents Morse code.

1843
Samuel Morse invents the first long distance electric telegraph line.

Alexander Bain patents the first fax machine.

1861
United States starts the Pony Express for mail delivery.

Alexander Graham Bell patents the electric telephone.

Loudspeakers invented.

1910
Thomas Edison demonstrated the first talking motion picture.

1914
First cross continental telephone call made.

1927
NBC starts two radio networks.

Searching it, understanding it, and using the insights of information space is at the heart of every person and company. Every start-up, including the criminal start-ups, who understand this strategy have an immediate competitive advantage; it is the 'new societal and business norm'. For current operating police organizations, where information and intelligence is the core of the business, it is even more challenging than for start-ups, because government has to understand the new norm and, at the same time, to unlearn previous procedures and processes; the dependency on information and intelligence growths with the growth of information space. Government is not excluded from this trend. Senior management must pay attention to how the business creates value in both the 'market place' and the 'market space'. The way they could create value is not the same in the two worlds though. Managers who understand how to master both can support the transformation in the most efficient and effective manner. For police business it means that the police must create an Internet production function to enable the organization to add values there.

1934
Joseph Begun invents the first tape recorder for broadcasting - first magnetic recording.

1938
Television broadcasts able to be taped and edited - rather than only live.

1939
Scheduled television broadcasts begin.

1944
Computers like Harvard's Mark I put into public service - government owned - the age of Information Science begins.

1951
Computers are first sold commercially.

1958
Chester Carlson invents the photocopier or Xerox machine.

1976
Apple I home computer invented.

1985
Cellular telephones in cars become wide-spread.

1989
Tim Berners-Lee invents the World Wide Web

1994
American government releases control of internet and WWW is born.

2009
there are over 400 million broadband Internet subscribers fuelling the global information system.

An historical view on Intelligence and technology

Intelligence is the second oldest occupation in the world. In the old days, Romans had a network of informants already. High ranked soldiers knew about everything in the cities and informants were getting paid to do so. There is nothing new in this era, but the dominance of intelligence has grown over the years. During the Napoleonic Wars, the French revolutionized land-based communications with the signalling towers bearing rotating arms to fashion coded signals that could speed, by line-of-sight from tower to tower across the country, at some 200 miles per hour. During the war on terrorism in Afghanistan, unmanned aerial vehicles, flying lengthy missions at heights of some 25,000 feet, have been providing surveillance of designated geography, installations, and activity. Today roughly a 1,000 informants browse through the city of New York in order to capture information and help the government with their 'war on terror'. Intelligence and technology are centuries old and always interlinked. With the rise of Internet surveillance, intelligence will change further; and it will be more dependent on light speed weak signals than ever before.

Forty years ago, there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are millions and millions of: networked computers (2 billion in 2015), cell phones (50% of world's population in 2010), fax machines and all kinds of connected devices and those numbers continue to grow. Today, exabyte's (10^{18} =10.000.000.000.000.000.000 bytes) of easily accessed data, always-on Internet connectivity, and lightning-fast search engines are profoundly changing the way people gather information. The telecommunications industry is making huge investments to encircle the world in millions of miles of high bandwidth fiber-optic cable, with one goal: to connect everybody, everything all the time. As from 1999, in only 10 years, the number of broadband subscribers to get access to the Internet has grown from 4 million subscribers to 400 million subscribers. At that pace every citizen around the world has a broadband connection before 2020. In this short amount of time Intelligence from around the globe is now somehow in the air we breathe, essential to our national security.

It also changes who is gathering information. In the industrial era only people with a specific occupation where gathering data. Now everybody and, in the near future, everything can and will gather, enhance and use information. It not only the information people put on the internet, it's also the meta data of people clicking and searching on the Internet and information that is pushed from things, like: cars, intelligent camera's, fridges, medicines and so on. Almost 2 billion clicks per day on the Internet, creates a 'thing' that is far more intelligent and much faster than human beings can ever be, and the machine is learning. Think how Google trends helped the US department of health predict

the flu epidemic. In 2007 Google predicted the flu epidemic 2 weeks before the department of health with its own super computers. Google's prediction was based on questions and search requests asked on the Internet. Nowadays people can build their own small intelligence application(s) and use the richness of the Internet and some open source application to get detailed information and alerts about a subject of interest. So memory, intelligence, becomes collective and individual at the same time. The undeniable democratization of information provides instant access to information and, in a sense, improving the practical application of intelligence for everyone. In the days of a life of a criminal analyst, it feels like losing the competitive edge. Everybody has the same information, and is challenged by the question of added value. So businesses in general must understand the upside and downside of the growing information space and change accordingly.

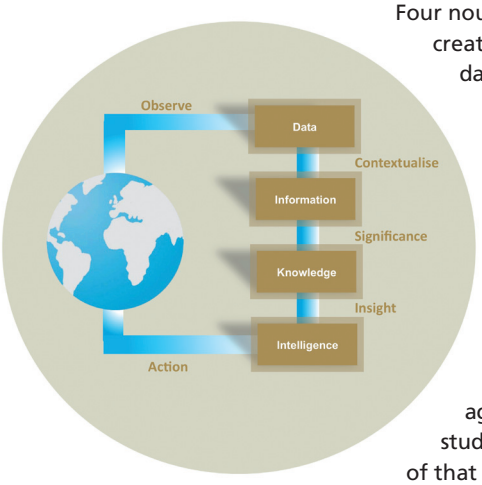
Intelligence in context

To define the term intelligence in a practical manner, it would be as short as 'actionable data' or 'actionable information'. Actionable is only defined inline with business goals. For the police 'actionable' means to find and arrest a criminal or to provide intelligence about dangerous crossroads. For a commercial company 'actionable' means information to bring in a large customer or to set the time to market.

The Internet era brings an on-rush of changes, both revolutionary and subtle, to the work of intelligence. It brings fairly big changes in the doctrine and practice of collection, analysis and usage of information. It will change the mindset around, intelligence, law enforcement and policy makers. In the current industrial era, police organizations still rely on informants and their internal data from crimes, crime fighting, research and day-to-day police work. This form of intelligence is based on covert, classified data sources and is just as good as the input of a small number of people and the data management on the sources. Especially for organizations dealing with criminals, frauds, terrorists and so on, the organization cannot only rely on a single data stream, because as a principle criminals don't tell the truth about themselves, their whereabouts and actions; it needs to be verified at all times. Given information space 'open source intelligence' must be carefully looked at.

Open source intelligence (OSINT) is an information gathering discipline that involves collecting data from public available sources[2] and analysing it to produce usable intelligence. Open source intelligence is one of the intelligence disciplines to be used by the police; it's certainly not the only one. Open source advocates the belief that a company can get at least 80% of what it wants from open sources. Open sources are: chat rooms, news groups, blogs, internet sites, web

portal, ecommerce sites, press publications, alerts, public magazines, academic reports, research publications, trade publications, open government policy publications



Four nouns need to be clarified before creating insights in the intelligence flip: data, information, knowledge and intelligence- [ref: dr. ir. M. den Hengst-Bruggeling]. Data is the raw material for information and intelligence. It is not classified and derived from everywhere. Data can be classified in three types of data. The first one is free and for free data. The Internet, libraries, open conversations, broadcast media, content aggregators, special databases, open studies and scientific work are examples of that type. Anybody can get this data for free. Second is limited access data, which contains all kinds of constraints like: legal constraints, geo spatial constraints and ethical constraints. Third and last is classified data.Classified information is usually limited to specific organizations, bodies, departments or individuals and shielded by laws or policies. Data is usually not directly usable for any intelligence purpose, it's passive and there is a staggering amount of it in all kinds of forms; especially on the Internet. The level of synthesis to create information or intelligence is very low and therefore raw data is not usable to make any decision on; it needs to be contextualised and analysed. On the other hand it serves early warning environments really good and usually gives instantaneous insight in a specific matter. The already mentioned example of Google predicting a flu, weeks before the health industry could do this, is a good one here. It is fairly possible that the health industry had data at the same time Google did, but didn't want to make any suggestion to a flu epidemic before they where absolutely sure about it. It's a good example of the difference of using raw data and being nearly right and using classified data and being completely right. The first one serves well in many cases of police work, but to arrest people or to intercept a terrorist attack it is absolutely necessary to right on time and to be absolutely right. Up to the 20th century, intelligence organizations were brought up with the idea of always being absolutely sure, working in secret and isolated environments and providing fully synthesised documents only. With the movement towards open source intelligence less synthesised information products on different sources prove their value also.

Data shifts into information when data is manipulated. Raw data could be contextualized, categorized, calculated, corrected, condensed, compared or connected to create information that is useful to an individual or organization. After manipulation it has a higher level of synthesis and the volume decreased. If information is not needed it automatically falls back into the category of 'data'. Information can be monitored or used for controlling purposes. Information turns into intelligence as result of the next level synthesis. Information is linked to business goals, consequences, chances, priorities and said to be actionable. The level of synthesis is high and the volume of intelligence is low unlike the level and volume of raw data. Intelligence can predict situations based on historical data and statistical analysis or it can diminish areas to search in by profiling on timelines, geographical areas, offenders or victims. For police purposes predictive models are very important for two main reasons. The first reason is that predictive models usually prevent situations from happening if the organization reacts intelligently to the results of a model, i.e. effective police action. Normally these situations deal will peoples' lives, health or wellbeing and are therefore very valuable to react on. If police organizations prevent such situations from happening in the first place it is a very efficient way of aiding public safety!. Usually to clean up the mess after a kill, accident or other unfortunate situation cost 10 times more capacity than to predict and act proactively.

In this transformation era police and governmental intelligence organizations need to rethink intelligence intelligently and redefine some fundamental paradigms.

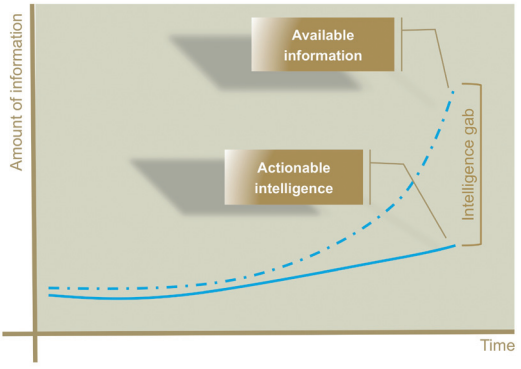
Intelligence moves from classified information towards open source based intelligence and from strong precise signals to weak and approximately right signals. The issue with this is that a much broader audience can have the same level of information. With the right set of tools and levels of synthesise even individuals can create a high level of intelligence. To rethink the future here is important to be able to obtain and sustain added value of intelligence organizations. Intelligence moves from isolated, single perspective organizational expertise to organizational intelligence. It's still definitely worthwhile to have a specific intelligence department, but to move towards an intelligent organization where the traditional linear paradigm from request to analyst, data collector and source must be replaced by a more non-linear paradigm where requestor, analyst, data collector and source are collaborating during the process of building intelligence. An intelligent organization aligns its primary processes around information and intelligence and work together with the intelligence organization to create even more and better intelligence. The third devolopment is defined around the level of analysis: from synthesized

analysis to early warning. In an information-dominated society where information is created and distributed with light speed and people are always online, early warning environments are increasingly important for intelligence-based organizations. Police management cannot wait for weeks and weeks to get the ultimate synthesised document of hundreds of pages. It needs a short and quick 80% precise decision supportive answer to questions like: 'when', 'where', 'who', 'why', 'so what', 'what if' and 'how to'.
The last fundamental shift is that the volume of information from electronic devices tends to increase exponentially. It is not only the word on the street or a set of selected and classified documents that provide the necessary information. All kinds of intelligent cameras, home security systems, in-car intelligence systems, traffic systems, financial systems are nodes in a network of intelligence information.

Intelligence flip

Intelligence is an important function for a police organization now and in the future. In general, however, the government is doing a poor job on intelligence. In most cases data and information are not treated as being key strategic asset to the business function. Sensing the environment and capturing data is mostly seen as an activity that feeds the bureaucratic control processes, instead of feeding an intelligent organization. Information processes that link intelligence and operational execution together are isolated and most information systems are not designed for creating intelligence, cross-departmental communication and collaboration. Finally laws, designed by people from the past era and focussed on a single dimension of privacy instead of global safety, prohibit a broad and agile collaboration.

The available information to create intelligence is now overwhelming. At first glance, it would seem that the age of the information revolution would be the best time for decision-makers to get the information and intelligence they need. The reality is quite the opposite because of: an information overload, too many potential sources to choose from and an increased aversion against technology capturing all kinds off data. Faced with these apparently insurmountable problems, decision-makers and, indeed, offices within



their organizations responsible for providing information most often make one of the following harmful choices: they either avoid the issue entirely, they rely on their own limited reading time to get the information they think they need or they create wholly inadequate products, such as clipping collections or news summaries. This results in an increasing intelligence gap and urges for a turnaround. Governments must at least evaluate their intelligence strategy to cope with tomorrow's threats. With the information economy at hand it's inevitable that information will be the key driver to change the business and drive mastering information as key asset for the police organization.

On the one hand the police is using Intelligence as a means to improve their efficiency and effectiveness. This aspect of the business grew from the paradigm: "I have information that you don't have and therefore I am better informed and can take a better of quicker decision". But the world changed, didn't it? Because the vast majority of information the police is taking their decision upon became general available information. Would the Intelligence function therefore change for the worst because of the global trends, or would the police organization accentuate Intelligence more and position it in the core of police work? One of the highlighted changes is that the integration between the business processes, information and the ICT function becomes stronger.

What does the intelligence flip encompass and what could the consequences be reasoning from this intelligence flip? In this text the word 'flip' means rather than to rely on the internal intelligence, the police needs to look at all the signals out there and complement it with external intelligence. With 2-3 billion information prosumers in the new global information space, intelligence 'flips' must be considered. In fact, if anything, external intelligence is better! Lets get back to the Google flu prediction example. Google was 2 weeks ahead of the department of health in this prediction, based on the intelligence derived from key words and search strings people all over the US used in Google! To put this in other words, the department of health, on which people rely on, was later than an organization working with information and intelligence. What does that mean for trust, legitimacy and added value?? Other aspects of the flip are described below.

- Intelligence moves from "the police knows more than you" towards "the public knows more and quicker than the police does". In this case the public is used broadly. If a closed intelligence organization looks only to its own information source it sees only a part of reality, there is so much more to see when the organization opens up. A Dutch Internet site like www.geenstijl.nl is also an instance of 'public'. Geenstijl, as company, gathers street information accurately and quickly. They are at the crime scene just as fast as the police

and releases crime scene related information on the Internet in minutes. Not just for fun, no way!! They find on the Internet over 300.000 amateur crime fighters from all over the country. Latest reports[3] on a research on civilians working in any way together with the police shows that over 80% over the population wants to be involved in law enforcement and crime fighting because safety counts for them. Although the validation issue of the information on the Internet needs a lot of thinking and discussion, the Intelligence community better get used to the fact that it no longer solely controls most of the information.

- In the public security value chain the police have always had a good information position, but if the public is starting to know more than the police, or any other national intelligence agency, then it is hard to keep up a valuable information position. The consequence of that could be that were the current value chain normally dependents on police information, it will flip towards a police dependency on external sources for information and intelligence. The police needs to clarify their competitive advantages against the background of intelligence.

- If again people have all the information at their fingertips, what is the competitive edge for the police against information and intelligence? In what way can they outsmart criminals and unlawful behaviour? The chain of custody and chain of evidence are very important concepts in that respect. The chain of evidence describes the quality of the crime puzzle put together by the district attorney and the police. The chain of custody describes the way this crime puzzle is put together and whether or not evidence is admissible in the juridical process. Advocatory will 'kill' the police organization in future if the police don't pay attention to these concepts, but the way to understand these concepts in the digital 'fluid' world of information space is really different and difficult. In this area the flip is that the police must have reliable and trustworthy information, better than anyone and that the organization has developed an organizational intelligence to embed intelligence into the primary processes and move quickly upon weak and strong signals. Organization Intelligence will be described later on in this chapter. Terrorist groups are, unfortunately, effective in their actions, just because they fight for their ideology and they are much faster than the government, military or police organizations are. So speed of information flow, focus on a target and quick a decision making process can close the gap. A new question in this area of competitive advantage must be: what are the chances that the new terrorists work from their home offices? And what damage could they do with the Internet as an instrument?

- The way organizations look upon 'data' as a concept will flip also. It flips from searching precisely to finding 'like', from strong one-dimensional signals to weak multi dimensional signals (mashup), from structured data in a relational database towards unstructured data in the cloud and from clean and verified data to dirty and unverified data with no single version of the truth. The police analysts will rather have multiple perspectives based on available data than far less data available within corporate data sources.

- Memory is the mother of all wisdom, but what is memory? Is it the person's ability to learn and remember culture, economics, entertainment, family, books and music? People feared the invention of the printing press because it would cause people to rely on books for their memory. But today, memory is not an issue anymore. If one is able to type 'Google', 'Exalead' or 'Bing', then the collective memory becomes available providing a practical intelligence base for everyone. With the Internet quickly becoming a mainstream medium of communication it is imperative to understand how the new intelligence must evolve in information space.

- The flip encompasses that the personnel the organization is using to produce analytics and intelligence is not directly the personnel that is up for the job, in the new connected world. Do they understand this connected world in its essence? Can they make real sense out of the information in a speed that the organization can organize actions upon? Sense making is one of the key valuables of an intelligence process and it's the most difficult ones. This requires a high standard of intelligence and peoples training and education. And are they capable of collaboration with a broad variety of other people and partners of this so-called value chain? In what way must the recruitment policy and the educational and training system change to meet new requirements; those of a connected world? What is the feeling and action of police officers and their management in the field towards these intelligence processes and information products? Nowadays it is really hard to sell intelligence to the organization responsible for law enforcement and crime fighting. The flip also encompasses that the organization needs to be setup to treat intelligence and information differently. An 'intelligent' organization is about agility and speed of action, strong collaborative processes, a focus on data and a drive for results. This triggers a redefinition of the information paradigm.

- Another big flip is that it is simply not going to work with the current proprietary information and communication technology stack, because of the information and communication technology organization, functionality, interoperability and openness to the new connected world. The information and communication technology organization must flip as soon as possible and drive information and communication technology from Internet as version 2 of corporate

information and communication technology[4]. The way the police organization treats information and communication technology, and everything with that, must change even more and, to be fair, even quicker. For upper management is often a 'thing' that cannot be understand, cost a lot and doesn't deliver at all. The orientation of information and communication technology must be open, unless something has to be closed and not the other way around. The Internet: cause and cure at the same time;

- Another aspect of the flip is that the way police organization is organised in different, and independent responsible business units, is not going to work. Centralising the organization, what most administrations would do to regain control over the police or budgets, isn't the brightest idea also. To define the flip in this aspect it would mean that the organization must follow the network orientation of the Internet community. Not with a number of independent police organization working freely together. To define it more broadly it has to follow the community structure and work together in the value chain and with the public. By working from a closed 'bubble' the police will not regain trust, legitimacy and added value. Another organization principal that will flip is the position of the intelligence processes and organizational structure that flips from being supportive to the primary processes towards being one of the primary processes.

- The governmental community faces the situation that it can no longer "muddle through" relying only on its legacy data and the knowledge of its managers. Focusing on internal data and information technology is not a path to prosperity. Instead focus attention on the next revolution of the development of an effective information system that provides functionality for the collection and organization of outside information. And last but certainly not least one of the bigger (cultural) flips is to take citizens and their behaviour on the Internet strategically very, very seriously if and only if management wants to own their business.

Is this the end state? No, obviously it is not! Since the information economy is changing and evolving, intelligence evolves also, because of the development in:

- Number of data sources increases. Each day a new source will reveal itself and be of interest to an intelligence organization. The number of web pages for instance grows each day, with each web page being a source of information. Criminals will use this information overload to their benefit.

- The variety of data sources increases also. It is not only flat and structured text, but sources become more and more integrated and multi-media. Capturing the key pointers from a text file is quite different from capturing

the key message from a 10 GB video stream. Let alone the hidden messages captured and processed within the video stream.

- The number of fixed and mobile Internet broadband subscribers increases and so does the number of netizens or prosumers. In fact the online intelligence community grows and it will facilitate communication patterns between people

- The governmental knowledge of crime and terrorist attacks increases over time. After investigation of the 9/11 attack and the attacks Madrid and London governments knew what data to capture and what to look for. Governments begin to understand that Intelligence alone will not save the planet. It will be a close collaboration of governmental bodies together with commercial businesses and society that will provide the new balance. Recognition of information value chain is the first step.

- Non-intelligence community members know a lot more than before and this creates the burning platform to deliver changes quickly.

- Emerging technology creates a whole new area for information led commercial business models.

These changes will mean a push to a specific form of organizational intelligence, which will be elaborated on at the end of this chapter. The type and quality of information analysts as well as the methods of analyzing evolve. It will shift from data collection and descriptive intelligence towards sense making and predictive intelligence. Analysts have to be open-minded, collaborative and network sensitive. They must never stop asking new questions on the job and get rid of taboos, prejudice and dogmatism. It is imperative that they work in a closed loop environment and use the 'collective memory' to their benefit. In a networking society, network intelligence (I know what you know as long as I know you) becomes more important and more valuable than the intelligence of a single network node. The police organization can be seen as a single network node. Network intelligence and social intelligence (the ability to get along well with others and to get them to collaborate with you) are being integrated in several communities. This process is supported by the easiness of transfer of knowledge through the Internet. These communities become communities of intelligence; participate or not? Current developments will also mean a push to the quality of data. In general the quality of data is poor, single dimensioned, passive, protected and based on strong signals. Data will evolve to be a key business asset and it will not only concern internal proprietary data, but open data as well. Open data is free accessible, transparent and a public good.

Commercial businesses will embrace this new line of work also. Information led businesses will provide either information products which can be used directly or peripheral services like identity management, intelligence software and strategic consultancy on topic concerning global intelligence. At the back-end of this change process, legislation concerning privacy and information security will shift. In the discussion after the prevented bomb attack on the flight from Amsterdam to Detroit (December 2009), the Dutch minister of internal affairs and the minister of justice started to investigate the usage of body scans at Schiphol airport. In the discussion about the privacy of travellers, the minister of internal affairs stated immediately that safety overrules privacy. This is a new statement in a new era.

To create managerial attention to the challenges of the predicted intelligence flip, management needs to focus on four major topics. Three of them are described in more detail. The last topic, legislation, is not elaborated on due to the complexity of the matter.

- Organizational intelligence
- Systems and functionality
- Data management
- Legislation

Organizational intelligence

Organizational intelligence [ref: R. Veryard] is a new way of looking at business improvement and survival, combining advanced software technologies with the latest management thinking to produce highly effective organizations. Organizational intelligence has been defined as 'the organisational ability to sense, make sense and act in flexible, creative, adaptive ways'. People and technology have complementary forms of intelligence. In an intelligent organization these abilities are coordinated and mobilized to the best advantage. On the other hand selecting the best people and the best technology don't pay any dividends for the organization unless the organizations overarching processes help connect them, promote collaboration and are open to feedback. An intelligent organization picks up and connects weak signals from its environment, responds in a coherent, timely and appropriate manner, communicates effectively across the organization, and learns rapidly from experience. In a volatile and competitive environment, only the more intelligent organizations will survive and grow. To achieve and enhance organizational intelligence typically requires both organizational change, in communication and collaboration, and technological change. There is already a proliferation of jargon: "agile enterprise", "collaborative networks", "enterprise 2.0" and "smart work".
What is the difference between intelligent organizations and 'stupid' organizations? Stupid organizations, which encompass the whole of people,

processes and technology, ignore important signals from the environment and lean on internal data only. They cannot discriminate between the important and trivial data. They respond incoherently and inconsistently to crisis and oscillate wildly between extremes. Strangely enough they fail to learn from mistakes and repeating the learned procedures over and over again. Less intelligent
organizations innovate slowly and painfully. Almost every change is a dramatic chain of events that creates high debts in the organization. Stupid organizations may contain very clever people (who don't talk to each other) and very sophisticated technology (poorly wired together) and reach the level of interference. For instance in the 9-11 catastrophe intelligence agencies had proper information on the terrorists, but the system, i.e. the organization, failed to put the pieces together and bring conclusions in time to the decision-making levels.
On the other hand intelligent organizations detect and interpret weak signals of possible significance and they mobilize coherent response to complex opportunities. These organizations have a more rational approach to risk and uncertainty, created high-quality decision-making throughout the organization and implemented collective learning and innovation by default. Intelligent organizations may contain good people (who work well together), good technology (that works well together) and reach the level of collaboration, where organizational intelligence is a 360°-system property. Intelligent organizations typically have many rich and diverse sources of information. Employees and partners actively contribute observations and insights over the borders of their own businesses and are able to tolerate multiple perspectives on what might be relevant. Organizational intelligence requires six capabilities. These capabilities will increase the pressure on information technology, because the amount of data used for analysis grows exponentially.

Perception and monitoring	How well does the organization collect and process information about itself and its environment? Intelligent organizations have many rich sources of information and employees actively contribute observations and insights.
Appreciation and sense making	How well does the organization interpret and understand itself and its environment? Intelligent organizations have clear conceptual maps and encourage critical thinking.

Reasoning and action	How effective are the (collective) processes of thinking, decisions, policy and action? Critical decision-making takes place closest to action; 'power to the edge'.
Knowledge and memory	How does the organization retain experience in a useful and accessible form? Intelligent organizations bring knowledge management, information management and information and communication technology management together.
Learning	How does the organization develop and improve its knowledge, capabilities and processes? Intelligent organizations innovate by doing and get time and resources to do so.
Communication and collaboration	How do people and groups exchange information and knowledge? How do they share ideas and meanings? Intelligent organizations participate in social networks and in collaboration networks. These are the place to find the most valuable intelligence.

Systems and functionality

The systems environment must support cross-departmental collaboration and the primary process with: collection, analysis, production, and dissemination of classified and unclassified data. Systems must support structured and unstructured multi-media data sources in data warehouses with sophisticated and mining functionality. Online access, profiling of search agents, statistical data analysis tools, imagery analysis and pattern recognition are key to successful intelligence as well as supportive functionality to modern communication and collaboration patterns. Important pre-conditions to create an agile communication across business s functions or even across departmental borders are: strong encryption, security (Jericho), data integrity, authentication, authorisation and language translation. This includes also attention to such issues as secure usage of the Internet, non-observable surfing, hacker resistance, intrusion detection, data protection, multimedia data fusion and audit capabilities; special attention to a modern solution of information security is key. Revisioning database concepts automatically tracks data pedigree including date of change, users, security information and data source information.

Data management

In many cases managers tend to seek new functionality to improve their information position or to improve their intelligence capabilities. In most cases the search for functionality is performed from one single business function instead of an integrated strategy. System functionality is nothing more than an action performed on data to create new data, information or even intelligence. In that respect functionality is important, but the underlying data is more important and yet there is hardly any focus on data management.
Data management is the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. In the modern information economy it becomes on of the most important business functions. Data management encompasses a whole range of topics to consider[5].
These topics are divided over non-technical and technical responsibilities. Normally business managers tend to push these topics to the technical responsibilities as if 'data' is an IT responsibility. Data is primary a business responsibility and mastering data will be enforced by the current information era developments. Strategic business management must get grip on data and data management. If not; the business will lose sustainability!

Data Governance	This discipline embodies a convergence of data quality, data management, business process management, and risk management surrounding the handling of data in an organization
Data analysis and modelling	Data analysis is a process of inspecting, cleaning, transforming, and modelling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making. Data modelling is the function to represent the real world into a conceptual data framework.
Database Management	This disciple is the more technological side of data management and keeps the data in the database up to date.
Data Quality Management	With this discipline data access and data erasure are covered.

Data Security Management	In terms of a database data integrity refers to the process of ensuring that a database remains an accurate reflection of the real world. In other words there is a close correspondence between the facts stored in the database and the real world it models
Reference and Master Data Management	This discipline comprises a set of processes and tools that consistently defines and manages the non-transactional data entities. In fact it is data about data.
Business Intelligence Management, mining and warehousing capabilities	Business Intelligence (BI) refers to skills, processes, technologies, applications and practices used to support decision-making. Data mining is the process of extracting patterns from data and a data warehouse is a repository of an organization's electronically stored data.

So what…

In an earlier part of the book the transformation and resulting paradigm shift was indicated. To redefine operative rules and organizing principles, for the police organization, is the question ad hand. It is difficult and challenging, but worthwhile to do and, to be truehearted, the number one responsibility of strategic management. In that respect the police organization MUST redefine collaboration. With whom is the organization going to collaborate with and why? What collaboration is going to stop; actively? The organization MUST also review its strategy for intelligence, information management and data management. Why is it so hard to understand the true value of capturing data and treating that information as an asset of importance? It has to actively redefine: transparency, legitimacy and trust in the new connected world. What do these verbs now and then mean to the organization and what does strategic management has to do with it?? The police must redefine innovation, because the old way innovation was treated is in hierarchy under maintenance of organization, processes and systems. Especially with governments the innovation process is not a mature process. In the new connected world this process is key to several results. The police really must redefine the aspect of openness and connectedness. There is no other way than to steer the redefined aspects of the paradigm shift into the organization. Needless to say that upper management and their administration will have a great deal of problems with understanding this, because from the organization they are the farthest from this new and

connected world. Indeed they are establishment and keeping it the way is has always worked before. The little secret is that 'the way we have worked before' ended. Finally, and there is probably more to redefine, it must redefine it's sustainability. It is not a project the organization is working on, it is a transformational shift into a new era with new rules and new leadership.

> If you want to create change, you must challenge not only the models of unreality, but also the paradigms that underwrite them."
> **Stafford Beer 1970**

---

[1] See Alvin Toffler
[2] Public available sources are non-classified sources like Internet streams, commercial feeds, commercial maps and images, academic studies, experts opinions, newspaper feeds; anything that is public available.
[3] The Dutch government conducted this research in October 2009
[4] See also chapter 2: The Internet Society
[5] Source www.wikipedia.com

4

POLICING IN DIGITAL SOCIETY

Chapter 4

Over the past decades police organizations have evolved from a semi-military organization servicing administrative and juridical tasks to a more society-oriented organization, in which people in the cities, suburbs, quarters and communities were the main focus for police work. Late 20th century, the police developed itself as co-creator of social security based on an integrated community based security philosophy. Police action alone can never free neighbourhoods from crime and violence. Nor by itself can it reduce fear. Only when law enforcement is viewed as an integral part of a fully accountable government structure, it will we be able to systematically create strong communities resistant to disorder and crime. Can the use of technology and the availability of information support these goals?

Normal 'off-line' communities are migrating in increasing numbers to a new dimension of information space that manifests itself outside traditional geographical and physical boundaries. The information space consists of purely social relations where interaction and community are performed at-a-distance. The diversifying populations of these 'virtual villages', towns and cities now constitute very real communities. The activities of a small and digitized group have resulted in a new type of crime that exists online. In just a few years the online communities have developed their own control and regulation guidelines and measures to maintain orderly 'communities'. This form of control emphasizes the difference between proximal forms of governing online behaviour and distal forms such as offline policing and criminal justice processes. The grand question is how these, often contradicting, nodes of governance interact and what the optimal form of interaction must be.

To answer these questions it is important to understand the concept of the word 'police' or 'policing'. The word 'police' comes from the Latin word 'politia', which means civil administration and the French word 'policier', both originated from the ancient Greek [pól.is] or 'politeia', which means '*city or surveillance*', 'city state' and also 'body of citizens'. State refers to a well-defined territorial jurisdiction, with its own set of laws and courts. A sovereign state, commonly also simply referred to as a state, is a political association with effective internal and external sovereignty over a geographic area and population which is not dependent on, or subject to any other power or state.

The police are people empowered to enforce the law of that state, protect property and reduce several forms of disturbance caused by an individuals or a group of people. Police powers include the legitimized use of force. Police services exercise the police power within a defined legal or territorial area of responsibility. A big part of the answer to the grand question of how to keep online behaviour orderly lies in the words 'territorial area' or 'geographical area'. All society and politicians have designed is bound to a geographical space, because previously there was no other space to commit crime available. Another pillar police organizations are built on, in the 20th century, are the Peelian-principles[1]. The most important principles to address to, in order to find answers to the grand question asked, are that the basic mission for which the police exist is to prevent crime and disorder and that the ability of the police to perform their duties depends upon public approval. The police must secure the willing co-operation of the public in voluntary observation of the law to be able to secure and maintain the respect of the public. To enable that, the police demonstrate absolute impartial service to the law of state and gives full-time attention in the interests of community welfare and existence.

Most important words to refer to are 'law', which refers again to a geographical area and 'community'. This is not an online community, but a real life community, as known for many centuries. In that respect policing in normal society is defined well, but the question lies inside the 'online' society, which is not bound to any geographical space or national law. How must the police then operate and maintain order in society? Is it a real community or not? In fact it lacks strong long lasting ties, proximity and a common history, which are all essential pasts of the definition of a community. An online community is also defined as a form of computer-mediated communication, an online social formation or a network sociality, all being devoid of history and based on the exchange of information, 'catching-up' and distanced relationships.

Online formations are second-generation multi-user domains. This second generation is much more technologically advance than the predecessors. The first generation was text oriented to execute tasks and support communication. Nowadays multi-user domains use optimal broadband network communications to locate each other and navigate through three-dimensional environments. This means that it will attract a much broader audience than in previous forms of the online community and therefore much more attractive to criminals. What is clear is that cybercrimes within these communities have 'real' consequences for 'real' people.

New technology enables new crimes

It is a given fact that the Internet introduces a various set of new crimes and terror attacks; the repertoire of a criminal is extended with another channel for crime-collaboration. Not instead of the old ones, but in addition to the old ones. Public safety partners have to prepare for new crimes and the possible international character of criminal behaviour. Emerging new crimes and terror threats are clustered as "cybercrime". This crime category includes: unlawful access to unauthorized computers, interception of unauthorized data streams, altering, deleting or disabling access to data that are processed by a computer and disrupting the proper functioning of a computer. This crime category includes also the attempt and complicity in relation to one of these offenses. As well as manufacturing and making available of instruments, software and other types of code designed for and intended to commit one of these offenses. Three different groups of cybercrime can be identified as points on a spectrum. At the one extreme are 'traditional' crimes that masquerade as cybercrimes. In such cases the Internet has typically been utilized for communication or information gathering to facilitate an offline crime. If the Internet is removed from the activity then the criminal behaviour persists because the offenders will revert to using other information sources or types of communication. 'Hybrid' cybercrimes occupy the middle ground. These are 'traditional' crimes for which

entirely new global opportunities have emerged. Take away the Internet and the behaviour will continue by other means, but not by the same volume or across such a wide span. A good example is the use and distribution of child pornography. At the far end of the spectrum are the 'true' cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace. These are the spawn of the Internet and therefore embody all of its transformative characteristics. Spamming is a good example of a true cybercrime. It results in small-impact bulk victimization. Take away the Internet and spamming and true cybercrimes vanish. Along this spectrum exists a myriad of crimes and misdemeanours.

The distinctions made between different types of cybercrime previously ('fake', 'hybrid' and 'true' cybercrimes) are important because the first two types tend to be subject to existing laws and existing professional experience can be applied to law enforcement regarding these offences. Any legal problems arising tend to relate more to the application of legal procedures than the substantive law itself. The final group, however, are solely the product of the Internet and pose the greater regulatory challenges.

Another way of explaining cyber crime is to divide it in two categories: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. Examples of crimes that primarily target computer networks or devices would include:

- Malware and malicious code
- Denial-of-service attacks
- Computing viruses, hacking

Examples of crimes that merely use computer networks or devices would include,

- Cyber stalking
- Fraud and identity theft
- Phishing scams, farming
- Information warfare
- Digital exploitation

A common example is when a person starts to steal information from sites, or cause damage to, a computer or computer network. This can be entirely virtual in that the information only exists in digital form, and the damage, while real, has no physical consequence other than the machine ceases to function. In some legal systems, intangible property cannot be stolen and the damage must be visible, e.g. as resulting from a blow from a hammer. Where human-centric terminology is used for crimes relying on natural language skills and innate

gullibility, definitions have to be modified to ensure that fraudulent behaviour remains criminal no matter how it is committed.
A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators. Some examples[2] are:

SPAM
Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful to varying degrees.

FRAUD
Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something, which causes loss. Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information

OBSCENE OR OFFENSIVE CONTENT
The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal. Many jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libellous or slanderous, seditious, or inflammatory material that tends to incite hate crimes. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with entrenched beliefs.

HARASSMENT
Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyber bullying, cyber stalking, harassment by computer, hate crime, online predators, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

DRUG TRAFFICKING
Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at Internet cafes, use courier Internet sites to track illegal packages of pills, and swap recipes for amphetamines in

restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. Furthermore, traditional drug recipes were carefully kept secrets. But with modern computer technology, this information is now being made available to anyone with computer access.

ILLEGAL COPYING
Criminals are interested in copies of credit cards, payment cards and access cards.

CYBER TERRORISM
Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them.

If society and criminals use new methods it's foreseeable, in fact inevitable, that the police needs to develop new counter measures and use at least the same technology as criminals do.

The challenge for public safety

Online paedophilia, cyber terrorism, identity theft, online fraud, malware infections, spam, denial of service attacks, 'hacktivism' and online hate crime, to name a few, have transformed the public's perception of the Internet from a new social space associated with unprecedented freedoms into a 'dangerous place' riddled with escalating, often misunderstood, risks. The public concern about 'cybercrime' subsequently shapes the demand for policing in cyberspace. But much computer-related illegality lies beyond the capacity of contemporary law enforcement. Social security in cyberspace will depend on the efforts of a wide range of institutions.

Online communities are plagued by variants of the cybercrimes and misdemeanours mentioned previously. Criminal exploitation of gaming artefacts in computer gaming environments, that have strategic importance in online role-play gaming, increases. 'Players' obtain artefacts that sustain their place in their games and help them progress through it. The artefacts are therefore highly desired because they represent not only high levels of ability and power, but also the hours of labour put into their construction. Because of this, players

are willing to pay large amounts of real money for them. It known that a virtual island was sold on eBay for over euro 18.000 in 2004 and in 2005 a virtual space station went for euro 65.000. Consequently, the high values of these artefacts have generated a string of new criminal opportunities. Already there have been examples of buyers being defrauded through e-auction sales, artefacts being stolen from players' accounts by hackers and even online mugging. Non-gaming-oriented communities also experience variants of cybercrime. Both citizens and tourists fall victim to harassment and textual, vandalism of private virtual property, identity theft, intellectual property theft, obscenity and profanity.

The challenges that these forms of offending pose for criminal justice systems are considerable, not least because the victims can point to real economic harms done to them through the illegal use, or sale, of their 'virtual currency'. A key question is how best to represent legally the loss in the victims' interests.

Most jurisdictions have legislation concerning thefts and provide legal measures for the recovery of lost assets, as well as intellectual property laws to protect against the unauthorized exploitation of intellectual property. 'Computer content' crimes relate to the content of computers; materials held on networked computer systems. They include the trade and distribution of pornographic materials, the dissemination of hate crime materials and the video publication of the murders of kidnapped foreign nationals. Once more, most jurisdictions have variants of the obscenity laws and laws that prohibit incitement, although their legislative strength can vary where Internet content is also protected by laws of free speech. In common with the other two crime groups, legislation does nevertheless vary across jurisdictions in terms of judicial seriousness.
A common characteristic, and first challenge, of many cybercrimes is that they lead to low-impact, bulk victimizations that cause large aggregated losses, which are spread globally, potentially across all known jurisdictions. Consequently, they fall outside the traditional Peelian paradigm of policing risk populations and capital offences, which frames the police–public mandate. Since local policing strategies often depend upon decisions made at a local level about the most efficient expenditure of finite resources, it is often hard to justify the 'public interest' criteria that would release police resources for the investigation of individual cybercrime victimizations.

A second and further challenge in inter-jurisdictional cases is the problem of *'nullum crimen, nulla poena sine praevia lege poenali*', which means: 'no crime, no punishment without a previous penal law' and is the basic of European legal thinking. The establishment of multi-agency partnerships and forums assists in facilitating inter-force co-operation, but they rely upon the offence in question being given similar priority in each jurisdiction. If a case is clearly a criminal

offence for which the investigation carries a strong mandate from the public, such as the investigation of online child pornography, then resourcing its investigation is usually fairly unproblematic. However, where there is not such an implied mandate, then resourcing becomes more problematic. Of course, the other inter-jurisdictional problem is that there may be cultural differences in defining the seriousness of specific forms of offending, or some offences may fall under civil law in one jurisdiction and criminal law in another?

Who should be policing cyberspace if the police are not? That is another grand question. Although the position of the public police has changed considerably since their formation, many of the original principles apply and need to be modernized as well. The basis principle remains to be: a bureaucratic re-active local force that maintains order and enforces law with officers who are identifiable from the rest of the public, professional in conduct, accountable to law and the community for their actions. However, the rise of the Internet along with its global, transformative impact creates a new range of challenges for public police, which challenges their traditional local dominance over the security domain and could in fact marginalize them completely. That is a big risk for the institution itself. Not only does cybercrime produce problems for the police because Internet-related offending takes place within a global context whereas crime tends to be nationally defined with policing decisions made locally, but policing the Internet is also a complex affair by the very nature of policing and security being networked and nodal.
The public police role has to be understood within the broader and largely context. It also helps to identify a broader range of cross-jurisdictional and cross sectoral issues that the police have to attend to in order to participate fully in policing the Internet, by fully embracing both the concept of networking and the subsequent network technology. This growing networking of sources of security, which includes police as a node, has become one aspect of the shift towards the networked society. A range of new transformations need to take place in order to enhance the effectiveness and legitimacy of a modern security architecture: A flattening of policing structures, parity of legal definitions across boundaries, broadly accepted frameworks of accountability to the public, shared values, multi-agency and cross-sectoral dialogues, and more.

New opportunities for the police

As described the availability of information, due to development in technology, will initiate a big shift in the way people live and work. Obviously there is a challenge for public safety as well. The 'new economy' brings opportunities on one hand and new uncertainties, insecurities and new threats, on the other. The increased wealth and education has brought higher expectation for public services; including policing. The traditional policing methods are expensive and

cannot be scaled indefinitely. It needs to change severely, but that takes time. It is perhaps possible to skip a few minor steps and put a big step forward because of the new opportunities the Internet provides; new threats require new responses. The professional criminals and terrorists are in general intelligent people and used to use technology to support their criminal goals. The police cannot stay behind in understanding and using this new technology in the core of their public safety tasks.

Policing has always looked to use new technological development to increase its ability to protect the public. Over the last twenty years, policing has seen major capacity development through the use of digital communications systems (including new radio systems), collection, management and analysis of data, for criminal intelligence and investigation, in command and control systems and in case work management. The ability to use technology to make sense of the information around us, i.e. intelligence, and to use that insight to fight crimes and prevent terror is an exiting new opportunity. The development of emergent and future technologies therefore presents new opportunities for policing:

EXTEND CITIZENS PARTICIPATION

One of the big challenges of modern policing is 'community policing[3]'. In the current organization it is difficult because it tends to be effective but inefficient. Nowadays organizations are more efficiency led than they are challenged on the effectiveness. The Internet can change that because of the easy and global communication functionality. An important part of citizen's participation is reciprocity. The fact that the Internet turns people into collaborating prosumers, supports the general idea of that. A good example of this is SMS Alert, where the police can call in the help of citizens to look out for an offender, a missing child or a stolen vehicle.

IMPROVED LAW ENFORCEMENT

If the Internet is the new world, criminal behaviour and public disruptions will find its way on the Internet too. Due to the openness of the Internet the police will face a new kind of criminal behaviour and will be able to execute the job in a different way. Not using the new opportunities, because of old behaviour, lack of understanding, mistrust will put the police organization behind. A simple example is to scan Facebook on photo's of known criminals or to superintend on specific issues on different internet sites.

IMPROVED INTELLIGENCE

By using meta-data on search requests a new form of intelligence will rise. When more police officers a looking for the same data, it means that that type

of data is more relevant. This relevance itself is intelligence. Look at the example of Google predicting a flue epidemic. Google predicted that epidemic not based on knowledge of flue and insights on the worlds flue spread, but solely on the search requests of Google users: medicines, doctors and hospitals addresses, symptoms etc.

IMPROVED INTERNAL COMMUNICATION

The Internet in general and Internet technology is enabling the communication between policemen. It will improve internal communication and it will personalize communication. For instance the police can use Twitter as a means to communicate. It may not use Twitter in the openness of today, but the functionality can be worthwhile. The usage of wiki's and other forms of information sharing will improve the knowledge of colleagues and enable them to learn and develop faster. This is not a 'nice to have', but a lifesaver in an organization build on citizen's trust. Personalisation means that the police officer can individualise his communication stream. He doesn't want to know it all but wants to be informed on available information on subjects of his interest.

USE MORE AND OPEN SOURCES

Police organizations in general use their own data sources. Most of the time that are two dimensional data sources with a minimum of links between the objects in other data sources. The number and nature of data sources has grown tremendously over the last years. Linked data is one of the key elements of the Internet in near future. Given the fact that 20% of the usable data lies within the organization and 80% is available on the Internet, it's key to restructure the use of data sources, because it can!

COLLABORATE SEAMLESS

The collaboration with citizens, corporate bodies and government can be improved by using the Internet and different social media on the Internet. Social security is not owned by the police, but shared with other partners and the public itself. Information and information sharing connects all partners seamless. Enforcing the value chain of social security will enforce the legitimacy of the police itself. Web 2.0 sites like Hyves, LinkedIn or Facebook can easily support collaborative work. Everywhere one can create groups one can communicate to groups.

SHARING OPERATIONAL KNOWLEDGE

For most police organizations it's hard to share knowledge, because there is no easy way to do that. A normal reaction would be to create an application to support that, but in most governments, that's difficult too. With all kinds of Internet applications supporting the communication between people, this problem fades away. To create a wiki is just as easy as to share information on the wiki.

EXTERNALISE BUSINESS PROCESSES

One of the major changes the police must go through, in using the Internet or Internet technology, is the ability to externalise business processes or corporate functions, to use information sources which have never used before, to personalize the work space of a police officer and create true mobility of work. By extending business processes the police acknowledges the fact that they cannot do it alone and are prepared to work together. It will be a great fundament for a shared responsibility on the public safety agenda.

TAP INTO COLLECTIVE INTELLIGENCE AND USE WEAK SIGNALS

The wisdom of the crowd is much stronger and more intelligent than a person, a board of directors or a company of any kind. Not tapping into collective intelligence would weaken your organization against those your work for; your citizens! Weak signals are very important in a society where agility, flexibility and pro-activeness is an important strength.

Major challenges in using new technology

It's easy to sum up all kinds of advantages using social media, flashing websites and connectivity. But it isn't easy to take advantage of it in order to really perform better in the government functions. Six major challenges have to overcome.

LEARN TO BE AWARE OF THE POSITION

In a network a police officer always has a different role. It's 7x24 and gives the officer a position to perform his tasks. A police officer cannot close his eyes when a particularly crime occurs in the network or people tell about crimes or give information about a crime that will happen in the future. At that moment he is a member of the police force and must take action.

GETTING OVER THE BUREAUCRATIC BUMP

Agencies need to realize it's not always the smartest person in the room. The most innovative person in government is being the one to use simple things with a big reach; like social media. The public needs to continue to push government for interaction and the first task for government is have leadership in place to set directions for the future. Looking at things like social media from a tactical standpoint, they're being used by the 'enemy'. If government doesn't have a handle on it, it is losing the game.

CONVINCING THE "MIDDLE"

In many organizations, leadership is on board with some of the innovations and in particular with social media, as an aid to communication. Youngsters

coming into these agencies are already tech-savvy naturals with Facebook, Twitter and connectivity. The problem often lies with middle management. They have been there the longest and they've got the most at stake. Obviously they're typically the most reluctant and resistant to change. In fact, the middle is often deliberately incentivised to improve predictability and to resist change! The trick is how to convince them of the value of social media to the way government communicates with civilians and not to avoid these technologies at their peril. What used to be the coffee machine discussion has become the crowd sourcing of solutions. It helped improve employees work atmosphere, empowered them as forces for change within the organization, and shown them the power of social media.

CREATING A TWO-WAY CONVERSATION

This is a problem not just for government but also for all users of social media. How *do* you create that two-way flow of information? What if your reputation becomes tarnished by comments on your Facebook feed? How do you monitor it? How do you convince people you are real?

The best way to overcome this is to try it and to start small. Governmental bodies must make as many of the social media available for trying and making their work environment better. The usage of social media needs to pas the smell-test between humans. It's all about the two-way interaction, making failures, learning and building trust. In that respect it's like a normal relationship.

MOVING FROM NEED-TO-KNOW TO NEED-TO-SHARE

During the Cold War, everything was on a need-to-know basis. Everyone was so paranoid and afraid of leaks and security issues that communication was absolutely kept to a minimum. Now, it's different times and no longer need-to-know. Society and government moves to a need-to-share environment, because information is now seen as a 'source' and a source that becomes more and richer by sharing the source. There are a lot of pros to this. Empowered employees, increased collaboration, greater openness and transparency, increased interaction with the public and bridging the divide between private industry innovations and government advances.

TACKLING INFORMATION OVERLOAD

By using these social media and having access to the wealth of information on the Internet it is easy to foresee that people will suffer from information overload. That potential disadvantage will drive them away from using it. In order to overcome this challenge it's imperative that people have to learn to use filters on their information feeds. Intelligent search engines will help in that process, but also the collaboration with early adaptors; research institutes and education will support the process of smart searching.

AVOIDING BLENDING AND POLLUTING

Especially in information dependent industries, like the police and the intelligence branch, blending and polluting information streams is a big disadvantage to overcome. Using information from all kinds of open sources to create a better information position is not hard to explain. Using the same information in a criminal file is much tougher. Criminal file information must but proven - and originated information otherwise it will not hold on court. The way the information was collected and captured and the originality of the information, normally called the chain of custody, are very important issues for the outcome of a juridical process against a criminal. Only having digital information at hand it imperative to set new standards for collecting and holding evidence.

---

[1] Sir Robert Peel, 2nd Baronet (5 February 1788 – 2 July 1850) was the Conservative Prime Minister of the United Kingdom from 10 December 1834 to 8 April 1835, and again from 30 August 1841 to 29 June 1846. He helped create the modern concept of the police force

[2] Source is wikipedia: http://en.wikipedia.org/wiki/Computer_crime

[3] Community policing is one of the key areas of development for the Dutch police and described in Police in Evolution, B. Welten 2004

5

MODERN POLICE ORGANIZATION

Chapter 5

Managing relationships and leveraging information in new ways can be seen as important trends of modern time caused by the development of the Internet. Both are meaningful in societal security because open and transparent relationships, communities, the exchange of information contributes a lot to security. Police organization though are build upon past beliefs, hierarchies, command and control principles and are ‘closed unless’ instead of ‘open until’. The light speed of societal - and technological changes create a hugh stepping stone for any organization. Policing in the future must be community based, intelligence led and supported by cutting edge technology. The grand question though is how to benefit from this available technology.

The way a police organization will develop in the future is complex. In general organizations will develop towards network-oriented organizations based on the primary products or function in the market or society. Hierarchical organizations are bound to the previous era of industrial society. Modern society is increasingly global and network-oriented. Examples of that network-oriented society are the explosive rise of social media, the shift towards core business and more intense business collaboration to deliver what is necessary and the whole view on safety as a collaboration between civilians, several departments and private companies.

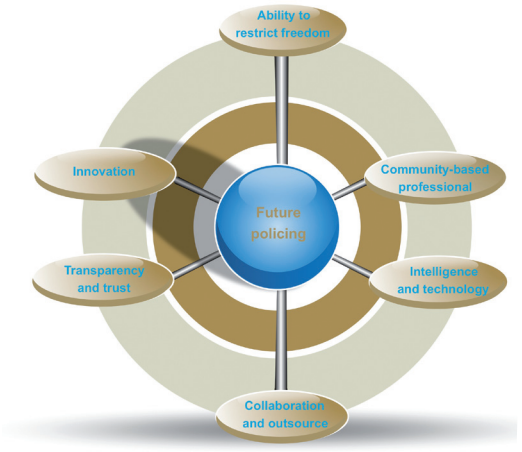
If the premise of network-orientation is right, what does it mean for the police organization, the business processes, employees and technology? It is for sure the changes will be huge. Society and organizations will change in the same intensity, these aspects changed late 19th century as the industrial revolution. To support all these new developments, and to stay ahead of crime, the police will have to use methods in terms of tactics, technology and organizational surroundings. New ways are found in spatial controls, social collaboration and technology based sensors. A lot of the new methods will be driven by new possibilities in technology. As stated before nano-technology and forensic sciences will rise in the next decade.

But technology does not only have a positive message and will have its downside. For instance the dependency on technology growth, the chance that technology will fail at a critical time will grow also. The trust in the police will decrease because of failing technology. Another aspect is that a police organization will need a certain "competitive edge" towards the competition, i.e. the criminals. If technology is the only edge on which the organization builds its advantage, it will fail. New technologies will also need new employees, new policies and new organizations and collaborations. The new police will answer to the consequences of the global trends of connectedness, information availability and the power of people instead of businesses. Resetting current paradigms and live up to the new standard.

Main characteristics of a modern police organization

Given the unpredictability of the future it is impossible to define future national policing strategies. However, based on current and anticipated developments a number of issues can be identified. A key issue is thorough reflection on the nature of the police's core business. With privatisation, partnerships and the multi-level approach to 'security and law and order all impinging on the policing function, it can not be taken for granted what policing is, who it is for and who will pay for it'. Development of the core business, adapting to all kind of 'flips', open source intelligence, knowledge workers, horizontalizing, networking with other parties and innovation are therefore key developments for strategic management to address.

It is crucial to be continuously aware of the interaction between local and global developments. Residents often demand a visible police presence in their streets. It will be hard for local citizens in an ordinary neighbourhood to understand why their police is, visibly, spending so much time on often less visible forms of (inter) national crime, while at the same time youths are vandalising their living area and affecting their daily wellbeing. In the future it will be a key challenge for the police to take on (inter)national crime without losing touch with local communities. With limited money and employees and a free 'product', as the police seems to have, it will be hard to deliver and to keep up the necessary legitimacy.



Given the above-mentioned aspect of future policing the current police organization must create at least the following characteristics in the modern organization. These characteristics can be seen as 6 levers to drive and follow through on the development of the organization.

The *first* lever is the police professional and self-organizing community-based police, or in future security, officers. Obviously the police profession is a complex and cool profession. This profession encompasses many aspects of crime fighting, law enforcement, emergency aid, communication and collaboration with citizens, businesses and partners. Who are our future police officers? This question is often discussed in terms of diversity and it is frequently said that the police service must resemble the society it polices. When they mirror each other there is less chance for the police to be or become estranged from the community that it serves. However, diversity is more than this. It is a given that a multicultural society requires a multicultural police service. The service must be gender balanced and welcome members from all faiths, ethnic backgrounds and social strata. In addition, a sustained effort is required to make sure that those recruited remain in the service, feel at home within the police and are offered the chance to develop them and receive career development opportunities. Or to actively manage the work force and to make sure that people leave the organization within a few years to make room for fresh blood. In that regard diversity is not so much about numbers per se, but more about occupational culture, attitude and strategy.

That remains one of the main challenges in giving shape to the police service of the future. The police officer must have or develop skills to work in a network-oriented environment, to work with information and intelligence and to use technology to perform outstanding. Future police officers don't work from an office and a territory, but work always together with other partners and society on social security issues. Each partner adding value to this issue using its own set of instruments. In that respect communication skills and collaboration skills are, together with the use of technology and understanding what outstanding policing encompasses, key to future colleagues. Command and control processes are changed into support and share processes. Professionals in any business do have the urge to be self-organized and want to take responsibility to perform a complex set of tasks and actions. In modern society command and control structures slow down result driven professionals.

The *second* lever to drive business opportunities is intelligence, technology and science. Police organizations need to keep abreast with developments in intelligence, technology and science. This book is filled with technology and the meaning of technology in the current era. Information and intelligence is key to cope with issues like legitimacy, trust and transparency. A new and modern organization with this lever at its fundament is also very important to attract youngsters to get into police work again. The use of science and scientific developments in the day-to-day work of crime fighting units is probably more important than new techniques of interrogation. In particular the use of collaborative technologies, information sciences and forensic science including profiling, predictive analysis, DNA comparisons, biometrics, forensic IT and so on. Due to the increase and mobility of crime, most police services will be urgently demanded to improve their results, without increasing the number of police officers, in dealing with criminal behaviour and therefore use technology to their advantage. Crime prevention and law enforcement will become more intelligence-led, so that the police will increasingly be required to manage information, rather than detect crime. The ability to develop an intelligence function in an open source global environment will be a challenge of all partners in public safety. It also requires new policies how to share information and how to use social media as an instrument of the daily routine. Technology is a driver for a sustainable police business and must therefore be well understood. The shift from 'best' to 'next practice' is a way to move forward.

The *third* lever is the ability to collaborate (network) and to outsource or externalise parts of current business processes. The traditional type of police service is that the police get a 'call' to service the public. This reactive approach is now moving toward community collaboration and pre-emptive problem solving. Instead of

driving around randomly in cars and responding to emergency calls, police are now working in their neighbourhoods. They work with community leaders to identify conditions that breed disorder; they share information about potential problems; and they forge common strategies for preventing crime, not simply catching criminals after the fact. Community-oriented policing reconnects police with the communities they serve. It has also breached the bureaucratic barriers that prevented multi-agency responses to the quality-of-life problems that facilitate crime, such as broken streetlights and abandoned buildings. Effective crime prevention requires that lights be repaired so that crimes aren't cloaked in darkness and that abandoned houses be condemned and razed so that they cannot be used for prostitution and drug trafficking. Thus, "broken windows" environments are eliminated before they begin attracting or reinforcing criminal activity. Even filling potholes is good policing policy it frees officers from directing traffic to catching criminals. Community-oriented policing also helps break down the stovepipe mentality of public agencies. It allows government and citizens to work together to tailor solutions that fit the crime problems in individual neighbourhoods. Emerging, cutting edge, information technologies such as wireless data and the Internet improve the delivery of government services. One very neat aspect of new technology that any business must take into consideration is the ability to redefine current business processes by using new technologies. In modern times police officers must master collaborative work as being the number one success factor of getting societal results. Collaborating with partners, communities, citizens, businesses and sciences are a few to mention. Not only building a smart technology driven counter to 'speak' to citizens or partners, but to set up mutual beneficial channels to collaborate; developing the right and effective collaborations is tough. Current organizations are 'factories' and therefore not designed for cross company collaboration. In fact every single body works within the hierarchy regardless of the better result when collaborating with partners. Future police officers must therefore strengthen mutual trust, relationships and interactions between the police and (confident) local communities. The police needs to participate actively in building and supporting the value chain of social, administrative and judicial processes. Working with empowered and communicative communities is likely to remain the bedrock of everyday policing. There is no doubt that effective community policing can occur only in partnership with community. Law enforcement needs to address both crime and the causes of crime through cooperation with partner organizations by preventing and deterring offending behaviour, and to catch, convict, rehabilitate and resettle offenders.

From a helicopter view this development can be seen as horizontalizing and linking business processes. This probably reveals business opportunities to outsource or even externalise parts of business processes to citizens and other

(new) partners. Nowadays the police organization is a patchwork of all kind of larger and smaller activities on public safety and crime fighting. The smarter question is in what way technology can help to improve results and to create a sustainable business mode again. Future police management must be able to see those business opportunities and follow through on that opportunity.
The creation of national and international centres of knowledge and excellence is a decisive matter. Such centres could engage in evaluation and dissemination of best practices based on commonly agreed indicators of crime. International policing requires a sound knowledge and evidence base and efforts need to be made to engender and foster that base; collaboration on an international level.

The *fourth* lever is the lawful right to restrict the freedom of citizens, business and partners and to use violence. Police officers can use violence or restrain individuals and crowds. The police can interrogate and tap into phone calls of use email logs to look after suspicious evidence. The police can search people for drugs or weapons and make arrests in order to maintain public safety. This lawful right is only given to military and the police organization with very strict rules of engagement.

The lawfull right to restrict freedom now and in the future will distinguish the police force from any other partner in the safety value chain. Controling the level of social safety is not only a matter of the police, but in cases of restricting freedom, other partners will always need the police to do so. Especially for controling heavy and organised crime, this capability is a strong 'competitive' advantage. In respect to this capability the police can even act against the will, timing or effort of other partners. Most European and American citizens live in a juridical state, where the police acts within the bouderies of the law, but sometimes outside the area of common interst. This lawfull right is a strong lever. Combined with the lever of intelligence and technology police forces must be able to cope with challenges of today and tomorrow.

The *fifth* lever is legitimacy, transparency and trust. For the global environment it is of the essence that international organizations are effective, well organised and transparent. It is furthermore crucial, in light of the 'act global, think local' and 'act local, think global' dual mantra that such organizations are trusted and valued by the communities they serve. Without trust from society, there cannot be an effective police organization. With that comes the requirement to increase clarity and operational consensus on the nature and extent of extraterritorial policing and police action in order to bridge security and enforcement gaps.

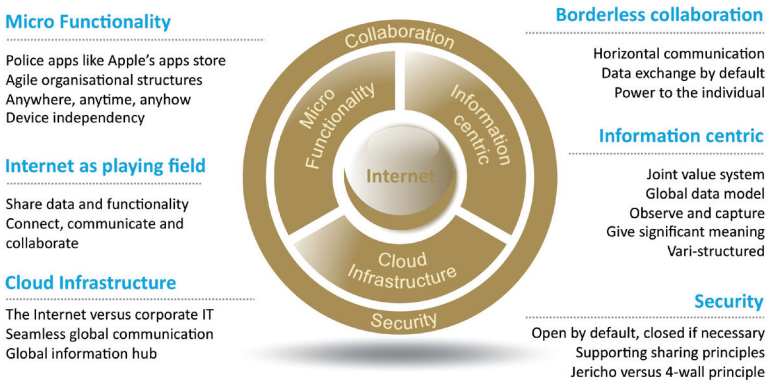
And last but not least 'Innovation' is the *sixth* lever for future police organizations.

As described before technology drives resources and in this era the Internet has driven the development of information as a key resource. Technology doesn't change over a lifetime, but changes more than once in a lifetime. This has an effect on people and their ability to change constantly. It has also an effect on the businesses in general because any business today must have a constructive, sustainable and flexible innovation process in place. Innovation is key to master current developments. Without innovation businesses fall behind and disappear. Governmental bodies will probably not disappear, but will suffer from a decreased legitimacy and trust. Upper management must support innovations on a corporate level.

The six main characteristics cannot be seen in isolation. These levers are not about the development of one aspect as a priority over the development of another. Not only to develop or strengthen the trust or technology lever. Not only to build intelligence as a product or process. But also to create a more intelligent organization, working with information and being connected to the outside world. The key strategy is to develop the six levers in balance, which will create a strong, mature, intelligent and sustainable police force. This must be appealing to upper management and the political administration.

The Information strategy of a modern police organization

Processes and process management are key components of today's business and business culture. These key components are highly developed from the 80th and have contributed significantly to the results of businesses, as we know it today. The world is changing towards an information-centric rather than process-centric type of operation. It changes from closed to open and from hierarchy driven to community driven. These are fundamental changes, which certainly affect various business aspects, including the Intelligence and the IT function.



An information-centric environment is driven by a number of *fundamental pillars* that must be fixed in the fundaments of its IT function. Basis of an information-centric environment is no longer the leading business process and information and communication technology functionality, but in fact the information itself and how it is used. Business processes where defined in the former era and, together with the organizational structure, they provide a rigid form of operation. To survive today it is better to focus on supporting communication and collaboration, than to support business processes. Business processes tend to focus on the boundaries of an organizational structure, whereas the company must work over these boundaries to provide the best policing service they can.

PILLAR 1 – BORDERLESS COLLABORATION

People do business with people. In community services communication between people is most important. Today's businesses and governmental body's are in a poor shape. Most managers don't get the point of the transformation and are not prepared to change pro-actively. They manage the operation like they have managed it before, only focussing on keeping things the way they are. So the first and utmost important pillar of an information strategy is to support very simple communications between people, groups and communities, inside and outside the company's borders. The success of Twitter is based on two factors: it gives power to the individual and it supports communication very simple. It is even that simple that you can use up to 140 characters to make a difference.

Collaboration and data exchange by default. The time that one single business of one single governmental body could work isolated and being successful in getting their target is history and will never come back again. Social security is a matter of collaborating and sharing data with many different and constantly changing partners. The exchange of data is key to success in the social security value system. The information strategy must support an efficient and effective, almost invisible, data exchange and at the same time be compliant to regulating information security and privacy laws. It must also not facilitate those people trying to misuse the information. The orientation though of data exchange is: exchange by default.

PILLAR 2 – THE INTERNET AS PLAYING FIELD

A dominant factor in a communication centric information strategy is to bring corporate information and communication technology to the web, i.e. pre-web versus post-web business and information and communication technology model. Pre-Web IT is characterised by a predominate model of applications and databases designed to support specific business processes and end-users

with very specific tasks and purposes, without any globally adopted standard for accessing information. Contrast the Web architecture (post-web), which is designed to support any user for any purpose, with a global standard for accessing information. These two worlds are colliding at the edge of the four walls of business and government and the new, connected environment they are seeking to adapt to. Decades of specific applications and databases on top of other legacy has not only resulted in a debilitating effect for a business to have a total view of itself, it is also hindering its adaptation to the connected global socio-economy. Often, 'users' in the business are now doing things for themselves by using consumer IT and bypassing corporate IT. Risks and missed opportunities are mounting. Businesses typically have a diversity of well-structured but incompatible data, and great investment has been made in systems (e.g. CRM, ERP) that substantially combine information from proprietary (non-open) systems. Achievable integration is resource-constrained, with limited opportunities for connecting to external data, which is in modern business models and key to deliver a sustainable service: 'to protect and serve'.

The Internet is changing all of this. It supports communication and connects people; this is what the Internet does. The Internet being version II of corporate information and communication technology; that is a challenge isn't it? And it sounds as a ridiculous and unreasonable statement! The cloud contains more CPU power and free storage than any company in the world. It is more a matter of getting to these sources and data security than data availability.

Furthermore the Internet contains a massive amount of free software, applications and services. Last but not least it holds an astonishing amount of information in all kinds of formats and sites. So the Internet has it all, why do we have corporate information and communication technology anyway? Two main reasons apply to this question. The first is that we have specific business oriented software. An example is software that supports forensic science or DNA capture and retrieval software. The other reason is security; the S-word with, in most cases, a capital "S". Due to history, culture, laws and management that wants to keep the company the way is has always been, security of data and privacy protection is and will always be used to conquer the value of the Internet; fear rules. The paradox is that the police organization stands in the middle of society, but doesn't want to use the same environment society does and keeps data to itself. Using the Internet as hometown doesn't mean that all information will be on the street. It means that once information is available it can be shared amongst everybody dependent on his or her authorization. In that way civilian's can enter a small part of the information for status updates. The police can access most of the data and partners can access specific data as well.

PILLAR 3 – INFORMATION CENTRIC AND REAL-TIME

Information centric and horizontal business models are models to collaborate with partners in a joint value system. It means working with other businesses and their unknown business processes. Currently data model techniques are tuned on 'four-walled' business processes and not on collaborating with other businesses. If the fundament of the 'four-walled business' fades away, the current view on data modelling must change. How do we know that we need a field to capture a 'skateboarding dog' in; we don't anymore and we don't want to be bothered about it whenever it happens. Google 'skateboarding dog' and you will find pictures of skateboarding dogs! That seems to be strange because nobody in Google mapped this type of data into a global data model; but it can be found, linked, used, copied and stored. In order to support a sustainable business the information strategy must support agile and flexible organizational structures. People – the best semantic processors on the planet – are making the links in harmony with the ICT of the internet. This is Berners-Lee's largest information construct in human history in action.Data is the source for information and therefore as important for intelligence as basic ingredients for a baker who bakes bread. If the ingredients have a low standard of quality, the bread will be poor as well. For the baker it will probably mean that he is out of business soon. For local – or national security and law enforcement the consequences of poor quality of raw data is more severe. Any information strategy must support behaviour, processes and technology to ensure maximum data quality. One of the levers for maximising data quality is the easiness of data capture and automatic input enhancement facilities. Any government must put emphasize on building cross governmental, unique and easy to access authentic data sources for individuals, companies, cars, criminals, households and other common data streams. In current society mobility of crimes is a common factor. European borders disappear and people travel in and out countries by nature. Data and information 'travels' with people and in 'time'. A modern information strategy must underpin the not only data, but data streams as well.

One of the most important functionalities is to observe and to capture data. Police man, or in future social security officers, need to observe sharp and specific and capture data quickly and efficient. Information technology can support that. The usage of small intelligent video camera's or the use of voice control support that process. The officer on the street must be able to capture data unstructured and one time only. The information stream can than be analyses and stored in the applicable applications or databases for later purposes.

Known data must be analysed into a significant meaning in order to support the decision-making process. Data is given significance by presenting data in a geographical area, against a timeframe or relationship diagram. Data is not only

analysed from a single discipline or context, but is analysed in a multi context and multi discipline environment.

The information itself is obviously important. Information is increasingly unstructured, multimedia and device independent. The representation of data must follow that. One of the key trends is that people and equipment will be connected. So all information, including social media, books, video streams and geo information must be made available regardless of the original form.

Data sources become more and more multi media sources. Flat text, photo files, video streams and all kinds of data sources and formats. This must become available for police officers, because that is the way citizens use information too. This means that new, unknown information based on location, date or tag is "mashed-up" and "pushed" to the end user. The number of data sources is countless, the new available data is enormous and therefore the user must be helped out with filters and push mechanisms to get the relevant data only. A mash-up is a set of layered data sources mapped together on a significant representation for the end-user. Information preferably is pushed to the end-user. By doing that, the police officer is always informed about his object of search.

The nice thing about a large company is that it can be considered one large community. A policing community is even larger because it is about safety and ties into all kinds of societal communities. If we adopt the idea that crime, terrorism threats and law enforcement is increasingly a matter of society, the community can provide a lot of potential valuable data. A specific police officer never knows what data has been uploaded from the community to the "police environment". Technology must support find, collect, mash-up and push mechanisms to support a police officer in his work.

Linked data is a promising technology. The definition of 'Linked data' at Wikipedia, Timm Barnes Lee, founder of the Internet as we know it: The Semantic Web isn't just about putting data on the web. It is about making links, so that a person or machine can explore the web of data. With linked data, when you have some of it, you can find other, related, data. This definition has great similarity with core police work. Especially with regard to crime fighting and solving crimes, intelligence and multidisciplinary emergency aid. The core would be to easily find and link sources, verify data, match timelines, present and share data elements and data sets. For instance when a crime has to be solved, the time line of occurrences and activities is an important factor, the specifics of phone calls or email and web traffic and the whereabouts of a suspect. A detective can only make sense of the separated data sources when these sources are linked together and presented in a nice and at that time suitable format.

Tagging[1] plays an important role in this way of working. Since linked data is the basic fundament for the Internet as Global Information System must this be also the fundament for an innovative information strategy.

PILLAR 4 – MICRO FUNCTIONALITY

Police functionality is divided into four categories: general business functionality, specific police functionality, intelligence functionality and communication supportive functionality. Most of the functionality can be retrieved from the Internet. Because of the level of specialism or the level of required information security, some of the functionality cannot be retrieved from any open source. The general business functionality such as workflow management, document management, financial management, personnel management and project management functionality can now or soon be derived from the Internet; no hesitation about it. Intelligence functionality, such as complex data retrieval, combining, filtering, (entity) recognition, analysis, reporting, mining, tagging, trend signalling, visualisation and representational functionality, can partly be derived from the Internet. The other part it needs to be bought and stored securely, because of the purpose of the functionality. The last category is the communication supportive functionality to support the communication in communities and tribes. That means to support the business with unleashing the wealth of wisdom of the crowds using all kinds of social collaborative networks, to support information retrieval from communities (network setup, face recognition) and to create a network interaction between all partners of the community. In any case a very strong precondition to open source software is that the data, on top of which the functionality works, needs to be Internet proof. If not, it will be difficult to use open source software. The other strong precondition is that the data retrieved from open sources is verified. It is dangerous in the security business to create intelligence and decisions on non-verified data.

The new architecture must be based on micro-functionality. Small functional units that can be used anywhere, anytime and always work on the same logical data and tied together with web services. Police offices can download small functionalities and work with that during their tasks at hand. The premise is that this functionality available on and through the Internet. The police must build a community of people, citizens and businesses, as 'developers' working on different functionalities. The precondition is that the police organization has its security policy in place. Functionality becomes available through a large number of devices, user interfaces and web services, associated with the logical data source. All of this functionality is underpinned by the data-centric architecture of the Web.

PILLAR 5 – SECURITY STRATEGY

Because of the openness of the fifth important pillar of the information strategy is the security strategy. This strategy must be chosen to ensure that the security is uniform and will secure data on the smallest item of information. Anyone with a specific authorization level can access data: citizens, businesses and institutions and chain partners and police staff. The real question is how to create an open environment. Nowadays security is a matter of closed doors, bridges and traps. Most companies use laws, detailed policies, large firewalls, encrypted lines, specific data centers for levels of security and a variety of logon procedures to ensure their data is kept and used security. The way security is organized now relates to the story of 'Bourtange', where the people are secure, but isolated. They could only innovate within the borders of their own small society, but didn't tap into the wealth of information, intelligence and innovations being out there. It is NOT to keep and use data unsecure manner, but to balance between security and openness. Security often has a user component in it, because rigid security can lead to end user problems in the easiness to enter or retrieve data. Security must support the end-user in the ease of entering data and at the same time to stay compliant.

PILLAR 6 – CLOUD INFRASTRUCTURE, ANYWHERE ANYTIME

Since society grows into a mobile society, technology must support that. A mobile broadband connection connects everyone in a mobile workplace. Mobile broadband is key to support societal mobility as the way forward. Mobile broadband is the name used to describe various types of wireless high-speed Internet access via portable devices. Mobile Enterprise (Mobile ERP) is a collection of Online Interactive Business Applications made possible by mobile broadband with the mobile enterprise platform in place, entire businesses can be moved onto the internet; the internet as version II of corporate information and communication technology, the new reality. Enterprise databases can be remotely accessed and updated from anywhere in the world, at anytime, with any device and by anyone with permission to access the service. These services are captured in the cloud in near future.

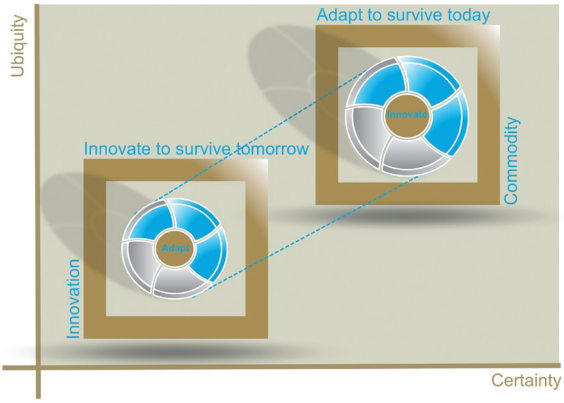
Leadership of change

An average human being consumes more information per day than a human being early 1900 in a life time; a radical shift in such a short period of time. Open, social and people are key elements in a connected world. Ultimately, the world is different today because a third of the world's people are connected to the 'largest human information construct in history', and global information connectivity is affecting all business, government and society.

Recent events have shown that the world is a less predictable place than we thought. Managing events within our own 'four walls' is, although still important

and necessary but also proving to have less significance than our ability to adapt to our external environment. It is not without irony that the very industrial specialisations that have helped create global connectivity are now barriers to us having a world-view across organizations, sectors and countries. This essential shift from an internal-out view towards an external-in view must be the newly required management focus. Coinciding with global unpredictability, information and communications technology gives us new ways of connecting – connectivity for more than half the global community is imminent. Therefore we must deploy new management practices based on agility, connectivity, collaboration and respect for multiple perspectives. It is no longer good enough to assume corporate control starts and ends with the four walls around it.

In this 'post-connectivity' world, business and governments are facing a triple whammy. Many of the old, business as usual issues, continue to persist; the old problems are still mounting up. So management must take care of problems and issues today as well as to develop new ideas for tomorrow. There is an increasing budget pressure in order to deliver more for less money. Finally there is a foundational shift in how both the organizations and societies share and use information.



The post-connectivity world demands new techniques in order to work within it. To manage all with one single technique or methodology won't work. It needs both 'to adapt to survive today' and 'to innovate to survive tomorrow' simultaneously at the same time [ref: Simon Wardley]. But there is 'an innovation paradox' behind it. To survive today it needs coherence, coordination and stability. To innovate and survive tomorrow it requires a replacement of these virtues. Most professional practices for business management and government were established before global information connectivity.

Organizations are increasingly finding that many of the well-known 'best practice' management techniques do not address the issues of the inter-related and inter-connected world. Some can even make situations worse.

The well-known leadership practices, developed and perfected before mass-access to the Web, are indeed best practice for walled organizations and for markets and societies where a few organizations are in control of the information to the many. But they do not serve the business or political leadership issues in connected markets and society. They are the pre-connectivity accepted ways of working. New professional practices, 'next practices', are needed for the post-connected world.

To enable the levers of the modern police organization and to implement the key pillars of the modern information architecture, upper management must change paradigms, set new business rules to coincide and interact better with information management and corporate information and communication technology, to be able to work in a connected environment effectively. Police management must embrace the Internet model by default and design. It will place the emphasis on people and information before process and technology to encourage information driven behaviour. Police management must establish an agreed, common and business-oriented language for business/IT communication, work collaboratively, move toward 'agile' delivery to support business change and bring innovation to serving business demand. Police management will institutionalise a problem solving mentality by asking who else (other industries) might have solved a specific problem before? Learn from the best is a good advice. Management must think corporate model first before IT model and make corporate strategy in a connected world top priority. Management must connect with external thought leadership communities and agile movements. It must always put the needs of the business first, work to regain the trust of the business and re-ignite the collective imagination. Finally management of all kind must see that the current societal development is not a technological development, but a people centric development enabled by technology. The shift from 'best' to 'next' is described in several aspects. [ref: C. Bate]

Shift from business process orientation to value systems. A value system is a coherent and coordinated set of activities, rules, policies, systems and information to meet a specific set of common goals between partners.

Shift from 'known data' to 'weak signals'. If 80% of the data is stored outside the organization, it is evident that the organization has to look for weak signals in addition to stored corporate data.

Shift from 'organization model' to 'network model and social capital'. The Internet is showing that understanding human systems is the most critical aspect of today's world. Before we had governments and businesses controlling information within a current organizational model – now it's open to billions

of people. The four wall vertical command and control policy is history. It needs to be replaced with a leadership working in a network and tapping into social intelligence.

Shift from 'theory X management' to 'theory Y management'[2]. Theory X managers assume employees are inherently lazy and will avoid work if they can (industrial model is based on this assumption). Because of this, workers need to be closely supervised and comprehensive systems of controls developed. A fixed structure of authority is needed with narrow span of control at each level; hierarchies rise. Theory Y managers come from the opposite perspective and assume employees are inherently self-motivating, open and that, given the right conditions, most people will want to do well at work. Theory Y managers tend to ask what they can do for employees, not the other way round. According to the Y-management, the X-management style leads to dis-economies, a lack of innovation and ultimately a lack of sustainable success. What's interesting is that the pre-Web organization has developed years and years the culture of business processes, process reengineering and enterprise resource planning. The Y-managers are getting more space to develop new rules, which are not constraint by four walled policies, but grow value systems.

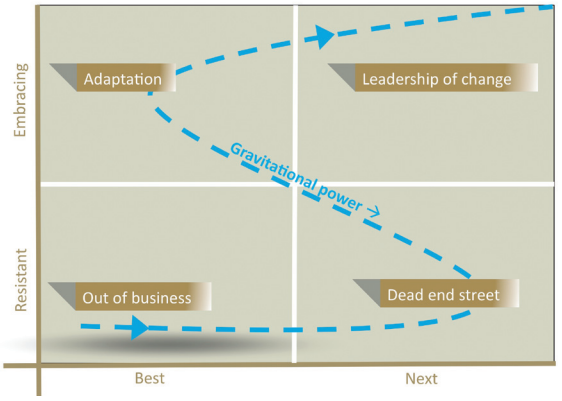
Shift from 'stability and predictability' to 'agility and innovation'. Under the assumption that current businesses utilize the global connectivity to add value in horizontal value systems, the organization is far more dependent on the way the systems behaves, develops and grows. To support those movements of a system the organization needs more agility, innovation and flexibility. The value chain itself must be agile while partners come and go dependent on their own business performance; wow, that's a two dimensional agility imposed on a hierarchical structure. With that also business planning will change. In current business models grand strategic designs, annual planning and change management are key issues to overcome each year. But due to required flexibility this must change towards adoption engineering and organic system planning.

Shift from 'four wall specialisation' to 'cross-discipline collaboration'. Again to be a specialist between the four walls isn't that great anymore in a connected world. If businesses are horizontalizing and become cross discipline anything within the company has to follow that.

Shift from 'divide between business and information and communication technology' to 'multi-discipline common language'. AS shown before information and communication technology is key driver of innovations. The current division between business people who don't understand IT people and vice versa must end; IT is business and business is IT.

Shift from 'users of applications' to 'participants in information systems'.
Currently almost everybody works at or with corporate applications, but are not tapping into the global information system. In the global information system, they are no longer users, but participants. The use and generate new content. The orientation therefore becomes external-in, which will replace the current internal-out orientation.
Shift from the Internet as bold-on' to 'Internet as version II of corporate information and communication technology'. If the existing business model and the way it organises corporate information and communication technology doesn't change, the organization will always be closed and lose essential fuel to innovate.

All these perceived shifts represent redefinitions of existing paradigms and must create the commonly know 'burning platform' for upper management. To change all of this needs leadership, consistency and a bright vision on the future to embrace these changes for the better. The path many businesses will follow, the model of gravitation[3], can be drawn on a grid with a horizontal axis from 'resistant to change' to 'embracing change' and a vertical axis from 'best' to 'next' as the figure is showing. In the four cells of the matrix the lower left cell means 'out of business'. The management of the business or governmental body has been reactive and keeps the best practise in place. It will not gain from the Internet and suddenly overnight some smart guys will overtake this business with another more intelligent and cost-effective model.



The lower right cell means 'dead end'. The management is pro-active, but still holds on a hierarchical model instead of a communications model. At the end young employees will see this kind of business as old fashioned and the business will not be influenced by new ideas.

The upper left cell means 'adaptation'. The management has embraced the new paradigms of the Internet, but still are reluctant to change or the critical mass

to change is too small. Firm leadership will get this type to the next level.

Finally the upper right cell means ‘leadership of change’. The best there is and something to gain for. It is hard to get there, but rewarding in terms of business value. The government must also try their best to get into this position. It is difficult to get from one cell to another, or to follow the path of development, because the forces against the ultimate change are very strong and often backed up by legislation. Management must realise that this legislation is created in the ‘best practise’-timeframe and therefore by definition not applicable to the new world. These forces act as a gravitational force, which pulls back the organization in the current or former phase of development. Strong leadership and patience can overcome this power.

---

[1] Folksonomy is a method of classification of collaboratively creating and managing tags to categorize content

[2] Douglas McGregor at the MIT Sloan School of Management in the 1960s that have been used in human resource management, organizational behavior, organizational communication and organizational development.

[3] Bate, Stiekema, september 2009 UK, London

6

IN SECURITY WE TRUST

Chapter 6

In many terms, but certainly in terms of security the Internet can be compared with a normal ‘in real life’ city. In cities there are slums, there are rich neighbourhoods, libraries, museums, art galleries, restaurants, normal buildings, places for entertainment and shops. There are also places that you don’t want to go: dark allies, dangerous suburbs and isolated streets and locations. Society is now breaking down barriers and the Internet supports this process of liberalisation. This ‘real life’ break down took decades of discussions, debates or decisionmaking. It resulted in a more open society. Society opens up and police organizations seem to fall behind. Slowed down by carrying the burden of a closed culture and many privacy - and information security laws prohibiting cultivating an open communicative organization.

The boundaryless environment hasn't always been present. Only a few hundred years ago, cities where designed to be closed with brick walls, canals and dikes to secure the people and goods in the city. A good example is the Dutch city of Boertange[1], an important fortification between 1593 and 1851, which was secured by a star shaped wall to disturb the supply route between Germany and the northern parts of the Netherlands and to protect people from the octogenarian war against Spain. People were secure within these four walls. The downside of this rigid secure environment was that the citizens couldn't benefit from anything outside these walls. They view on online security like the view on security of townships in the 16th and 17th century: save inside and closed to outsiders, closed to the wisdom of the crowd. Society has to learn how to deal with the Internet as being a digital 'town' to ensure that everyone can live and work online with confidence and safety.

Many years now government has brought up management to find confidence in a closed environment. People did trust a technological solution to seal of an organization from outside influences. It does seem to get crazier, just because of the Internet and the increased level of digital attacks and identity theft. It plays into the hands of established IT risk management and it enforces current perimeters. The cost to secure data increases rapidly. To continue this path will be a dead end street, so it is wise to approach security and trust from a different angel.

In the pre-connectivity era the prevailing opinion was: "knowledge is power[2]". Most information was flat text instead of multi media. Information was stored in several small isolated databases and the value of information wasn't discovered and valuable information was not shared; even not amongst colleagues. Individuals tend to keep information to themselves in order to benefit from it individually. Due to connectivity the opinion shifted over the years and is now being replaced by the opinion of: "sharing creates value[3]". The reality of that is shown on the Internet where almost everybody shares information about themselves, his or her hobbies and whereabouts. There are a couple of different ways to share information. Sharing inside a police organization or a governmental body is nowadays not as a big issue as it used to be. Personal preferences challenge the concept of sharing now and then, but when individuals see that they benefit from sharing, they will start sharing information themselves. Sharing between governmental bodies or partners in the safety chain is still a problem. People find it hard to take responsibility for sharing data and act by strict following the privacy - and information security laws. This is rather strange considering the fact that a value chain normally has a common goal to achieve. In working situations more and more 'information sharing'-convenants are being used to smooth the process of information exchange.

The exchange of information between any police organization and the Internet is mapped on a grid between the sharing direction and the level of interaction. The sharing direction can be internal or external. The level of interaction can be individually or mass interaction. 'Inward sharing' is sharing internal information with individuals from governmental bodies through specific and secure applications. 'Outward sharing' is defined as sharing information with external groups within the government. Outward sharing includes also public websites used in a private function to facilitate the information-sharing task. 'Inbound sharing' is also known as crowd sourcing. The government for instance asks the public to participate in an online meeting. Finally 'outbound sharing' refers to the governmental engagement on public commercial social media.

The distinctions and perceived goals need to be fully understood because the use of the Internet, i.e. the use of social media, and the subsequent concerns, form a complex topic that involves not only familiar threats, but also introduces additional vulnerabilities requiring updated sets of control. To mention a few 'new' vulnerabilities: spear fishing, social engineering and web application attacks. Spear fishing is targeting at individuals or groups to deceive them into performing an action that launches an attack. Spear fishing relies on knowing a piece of personal information such as an event, travel plan or a general interest. With that information spear fishers build a 'trust' relationship. Spear fishing on high-value individuals is called 'whaling'. Social engineering relies even more on exploiting the human element of trust. Social engineers first collect personal data about the 'target'. Social website reveal enough personal data including pictures, home addresses, phone numbers, work location and interests to use. The second step is to use this personal information to a 'target's' friend to elicit even more information. Social engineering on targeted groups is called 'social networking' used to give insight in a social network environment. Social networking on a police force could lead to loss of effectiveness of the organization or a crime related case. Finally web application attacks are an attack from a web application granted access by a targeted individual or group through a social website. Facebook for instance uses a wide range of web applications from which most of them are trustworthy. If a malicious web application attacks the government it could lead to posting information that seems to be authorised by the government, i.e. intrinsically trustful. By encouraging citizens to use the information or to click on the information it could easily lead to an avalanche of attacks. Looking from this perspective 'sharing information' in an information economy therefore is a strategic business issue. Senior management must take measures in order to share information safely. These measures include technical - and non-technical (behaviour) controls, which must been taken seriously and followed through in order to protect valuable information and the performance of the organization.

It is legitimate to state that almost every aspect of breaking out of this isolation is in place. The only thing that keeps governmental bodies to do so and to exchange information freely or to tap into the wisdom of the crowds is legislation and trust, whereby common trust models in fact have driven legislation in the past. Setting up a new trust model creates a new perspective to lawmakers over time. This legal construct around information is based on the lack of trust, or trustworthiness, and the grand fear to be unable to individually control information with personal details. The latter could easily lead to misuse of that information or even to identity theft, whereby identity theft is one of the fastest growing criminal activities and must be monitored and fought against from an international perspective. In a way the current legislation is not only hampering governmental connectivity, it enforces also the current risk management, which indeed pulls government away from connectivity.

The Internet provides people with an instant 'boundary less information flow' without any decision-making or any cultural or social behavioural change and people love it. Opening up in the digital world means more than the opportunity to share your Facebook with friends. There will be a dependency on digital communication, massive interference on existing processes will be a 'new era'-ability and new crimes reveal themselves on the Internet with people's identity as an important target. In that respect opening up towards a boundary less information flow needs a big trust! It probably needs the same decades of debates as it has had in the real world and it needs to be done intelligently. The risks need to be fully understood, or gradually changed, in order to shape societal behaviour that suits a boundary less information flow. The orientation of this discussion must be towards an open society, because that's is the new reality.

Where security meets trust

The key word used is always 'security' and the concept of security has the edge of being closed, isolated or secret. In that way information security is always connected to 'no', 'stay out' and 'don't use' and it is used in a broad rough sense, instead of using information security as an important (business) function in four dimensions: to secure specific data to specific users on several security levels in time. Security is not about preventing information to flow, because that is an unreality in our connected world. But strangely enough the most implemented and broadly used supportive technologies are indeed based on preventing information to flow. Firewalls, password policies, LAN separation and laws are not designed to facilitate the ones who need to be able to share data, but are designed to shut of and isolate a governmental body from the rest of the world. This will not hold for long!
Computing history shows an increased connectivity over time, starting from no

connectivity and developing to the restricted connectivity we currently have today, with islands of corporate connectivity behind their managed perimeter. The separation between the Internet and the police organization, or many other governmental organizations, is the firewall; a piece of equipment that prevents open communication. The firewall prevents hackers to come into the closed environment, but it also prevents the police to hook onto the wealth of information, bright ideas and new concepts of the Internet; a true dilemma.

The current perimeterised architecture is perfectly adequate for an organization that simply wants to operate inside its own controlled environment, with e-mail to the outside world. Unfortunately this organization ceased to exist years ago as business mandated wider connectivity. Yet most businesses continue to use an architecture adapted from that past era thereby exposing them to an increasing and often unwise risk. Security models designed and trusted pre-connectivity, may no longer work; but corporate bodies know these models and trust on them; no aspect is more misunderstood than this one. Each and every opportunity that comes along, establishment will enforce the current and rigid beliefs around the Internet and security models and enforces hardening the perimeters. Worst still, many business and IT leaders, who rightly understand that good security is mandatory to do business in the 21st century, have become victim to the perpetuated myth that good security starts, and in many cases ends, with a hardened perimeter, and also the fallacy that a hardened perimeter is required by whichever audit regimes they are subject to. It is essential that businesses and IT leaders relinquish this preconception, and understand what their businesses would be able to achieve if the perimeter was not there inhibiting innovation, wide collaborative working, expansion and effectiveness to society today!
The connected environment requires big leaps in the way the police defines, thinks and acts. The sustainable vision is indeed that sharing information is the key driver to grow the potential of current police organizations. The cloud is the future opposite of corporate information and communication technology; a clear and vivid vision to pursue, but difficult to explain to people raised in a corporate mistrust. Open source intelligence will play an important role to police intelligence of the police organization in near future. For all of this to happen, current police forces are evident to be in need of a trustful, agile and intelligent organization, which is typically not the fact for police forces and political administrations throughout the world. Last but not least: this is a business issue and not an IT problem. The move to a digital society changes governmental services and that requires fundamental changes in general belief structures, policies, regulatory, legal frameworks and applied technologies around online security; common paradigms about trust, security and legislation need to be redefined!
One of the paradigm shifts is that the government accepts that current informa-

tion security, despite all efforts and money spending techniques, is far from secure. In any random governmental body a malevolent employee can get so called secured data and share that with people interested in that data. Using portable devices to steal information or enwrapping techniques to use the benefits of the information infrastructure to send information out are examples of that. By the way criminals and terrorist groups use these modern technologies broadly! Fortunately not many employees are familiar with effective theft of information. Unfortunately many decision-making bodies are not aware of the risks involved or the opportunities they miss to grow their business. The transformation is to change the security policies from isolating principles towards "de-valueing" information. In fact it is a shift from securing information infrastructure towards securing information itself. By securing information infrastructures non-authorised people cannot enter the environment that holds the information, but once they are in, they can shop around. This is quite easy to execute. Securing information itself means to support broad and boundary less use of the information flow for authorised and authenticated users and it devalues information to non-authorised users. Data can be devalued by using encryption and scatter techniques.

The other paradigm shift is to see security as a vital business function coming out of a defined business (or governmental) vision, instead of a technological facility. If the government has the vision to have citizens participate into governmental processes, policymaking and information sharing, than it is absolutely vital to adapt security as a business function to unroll a citizen-centric strategy. Not in a way of telling people what they can't do, but what they can do and build trust from the fundamental business vision. In order to enforce the relationship with citizens the government must implement a broad and solid business-architecture to support that. There are a lot of technologies to secure and perimetise, but technology is merely one of the indirect aspects to create trust in an online society.

Trust models

The common ground is around the new reality of information connectivity, and that the police, and other government organizations must find ways rapidly to establish trust in it, or be overwhelmed by it. The first step is to acknowledge information connectivity is the new reality for society, government and commerce, and the new unreality is continuing to operate a model designed for pre-connectivity.

For centuries, the majority of society has sought to overall increase connectivity, rather than decrease it. The drivers can be found in many places, but perhaps Maslow's hierarchy of needs explains things straightforwardly enough – from

finding alliances to bring security, to trading to secure food, to communication between like minded people to share ideas, to trading to secure wealth and recognition, to exploration for its own sake, connectivity seems to be a natural side-effect of our reality. Technology has always tended to increase the support of that natural drive to connectivity; language itself, modes of transport (land, sea, air), the telegraph and the phone, financial engineering to enable globalisation of economies, and now the Internet.

The information strategy of the government hasn't fundamentally changed much during the described march of connectivity. To enable its people to share in benefits available to them, in this case through connectivity, it is important to set new rules. With each new type of connectivity, new trust models have had to be developed. Now is the time to do this again. The question therefore is not if but how fast society breaks down the old belief structure around security. Secondly, whichever way anyone looks at it, any government needs to balance security with the cost attached to it. It might simply no longer be able to afford current IT delivery security models, at least to the same degree as it has over the past decade. And so the real question to consider is, given society have had 50 years of experience of gaining trust in the strengths and weaknesses of corporate IT security, but only 5 years of experience of the Internet: how can society gain a majority of trust in the new web-based security models and how can we do so quickly? With the speed of technological developments, innovation and the speed of 'soft' changes has become essential.

Trust is defined as: "willingly relinquish control, making yourself vulnerable to someone else for a certain outcome or consequence" Trustworthiness is defined as being worthy to receive the trust from somebody else. Trust grows as a result of positive experiences accumulated over time. There is no reference whatsoever that the police can trust the Internet or society can trust the police in dealing with large amounts of information, simply because there haven't yet been the experiences. How does society than accelerate the general understanding of new security models in the new reality of global connectivity?

Rethinking common trust models means trusting the wisdom of the crowd as well as one's own intelligence, or it means trusting information-centric security and the emancipation of privacy control models. Fundamentally, it means to trust people. Because information connectivity, people must learn how to trust or distrust other people without a government telling them who to trust. In fact, the more closed a government, the less people trust it, and the more they find trust in other people and other opinions. The police need to learn how to be a leader in the new trust, or their effectiveness for public safety can only reduce. The organization needs to grow from a technological driven security

model towards a value driven trust model. Trusting that by opening up to the society they serve, its agencies can become stronger.

In that respect is legitimacy the rock hard reason to break out of this rigid pattern of isolation and to redefine what the term trust means to the organization. Legitimacy is roughly the societal support for legal actions. If the police organization isn't trusted in their actions against civilians, the legitimacy decreases and with that the power of action from the police decreases. A downward spiral emerges. Legitimacy and trust are interlinked, but there is more than one trust appearance the police organization has to take into account [ref: Richard Veryard].

AUTHORITY TRUST
For many citizens, the police force both symbolizes and realises a form of social authority. This authority is reinforced by police procedure, and by wearing the uniform. Members of certain communities or subcultures sometimes have a hostile attitude to this authority. Defence lawyers may attack police procedure in order to undermine trust in police evidence. One of the key objectives of the police is to provide evidence to court. Evidence can be hard forensic evidence or a data trail. In any case the 'chain of evidence' and the 'chain of custody' needs to be in a fairly good shape. These lawful concepts need to be translated into a digital world.

NETWORK TRUST
The police don't operate in isolation but in collaboration with other bodies such as social services, health, education and the judiciary, as well as community groups. Trust in the police force depends on complex institutional and often semi-formal arrangements with these bodies, and may be affected by problems elsewhere in this network. To be a true partner one must create a solid and trustful information exchange environment. Each partners needs to be willing to adapt and to be reviewed, but also to review the quality work other partners are doing. Only then the value chain will strengthen.

COMMODITY TRUST
Trust in the quality of service provided by the police. Service targets - crime rates, crime clear up rates, speed of response. If these services meet the expectation then the trust in the organization will grow. One of the more annoying aspects of current time for establishment is that not only the government can provide internal data; society can emanate the same data through the Internet.

PERSONAL TRUST

Trust created by personal relationships between individual police officers and the community. Do people feel confident to speak to a police officer? Does he have the right skills to tackle the problems ahead? In the digital world police officers also need to be skilled in the art of the Internet. That needs a completely different skill set.

To trust the connected environment is not easy; it is not a switch to turn on or off. Trust is a complex of different elements and characteristics divided over a few trust appearances. When the police feel confident to trust the outside world, individuals or communities, it addresses the subjective element of the trust model. It feels that it is okay to receive a mail from somebody or to use an Internet address because the information on the provided web site feels trustful. The objective element satisfies the organization with measuring the trustworthiness of data. It is driven by facts more than a subjective feeling. It also addresses the way management treats this subject to their subordinates. Nowadays management is fearful towards the Internet and subordinates do see the potential of it. But because they are not part of the management circle, they hesitate to use the Internet to its fullest potential. Or put another way, to really engage in the new reality. Having made the decision to trust the 'outsider' the police needs to proceed and trust in some action. This could be with a task, or with a confidence, certainly in some format that would serve as a building block to a long term trust-based relationship. And as in normal human interaction the loop back is important as well. It is then good to reflect on the outcome. If the outside world has proven to be trustworthy and gained a satisfactory positive outcome, it will build confidence. Over time, these positive experiences will serve to grow trust in a digital society. This is a time consuming process. In some cases it will take time to the next generation of management to establish the right level of trust.

Furthermore trust is build out of 6 interrelated characteristics. The first characteristic is *dependability.* In order to be considered trustworthy, you must be able to demonstrate that others can depend on you and can rely on you to do what you said you would do. Police forces are mainly inside-out organizations. Citizens do not 'feel' the interdependency and are not likely to trust. The second characteristic is *integrity*. This means always doing what you say you will do - always speaking the truth for the other's greater good, and never intentionally misleading other people. The third characteristic is *credibility*. Credibility is also about your professional ability to achieve what you promised to achieve. How often can a police officer depend on the quality of his environment, or the network, to make sure that he can make his promises come true? The forth characteristic is *empathy*. It is the power of imaginatively

entering another person's experience and conveying this to the other person so they know that you are travelling with them on this particular journey; empathy produces loyalty. The fifth characteristic is *self interest*, whereby self interest means not always being motivated by getting your own needs met, rather being motivated by meeting the needs of the client. Greed is often a powerful driver in self-interest. The sixth and last characteristic is *consistency.*

The big question though is how to sustain legitimacy in the connected world and self-created isolation most police forces are living in. What paradigms must shift to enable to open up in near future and which partnerships and collaborations does the organization need to enforce that? And which actions have to be taken? Normally they are: acknowledge the problem at hand, envision the alternative solutions, set the pre-conditions for the organizational change, take massive action and follow through consistently. To start with the pre-conditions it is obvious that upper management needs to create the ability to work inside the cloud. To do so business management must have a clear:

- Vision on the corporate information function, and their target groups (customers, citizens) they work for, derived from the general business vision and strategy;
- Understanding of the classification of corporate data. Without that there is no way to create an open environment;
- Understanding on how the Internet works and what the benefits and pitfalls are;
- Vivid collaboration with network partners from a common perspective on the Internet;
- Understanding on regulatory issues concerning the free flow of data;
- Set of controls implemented to filter out the negative side of using the Internet;

Where agility meets trust

The lack of sustainable agility can be traced to a loss of trust. Trust is critical to the proper functioning of an agile organization. Where there is less trust, we see more dysfunction. On the surface it can appear that everything is going well, but it is second nature to put on a façade of trust. Ultimately the effectiveness of a police force or a network of collaborating partners will reveal how much, or how little, trust actually exists. Trust is slow to build, and quick to destroy. Since trust is a basic element of agility, the nature of trust makes agile fragile. However, there is hope as well. Trust relationships exhibit plateau behaviour. Once established, they achieve a degree of stability that allows trust to survive sort-term attacks. A slow erosion of trust, or a catastrophic trust-breaking event, will still lead to dysfunction. If you are feeling a loss of agility, it may be a good time to check on the level of trust in the organization.

It is important to define what agility actually means to the organization before getting on to how an organization might achieve it. Does it mean: speed to market, speed of reaction, foresight, adaptability or the ability to change the rules of the game yourself? Often in these situations it can be helpful to get the dictionary out where it is defined as being ‘quickness of motion’. Recent global increased terrorist attacks and criminal development have put the spotlight firmly on agility again, and the ability to react to unanticipated events. In unusual situations, times of increased risk, we tend to rely more than ever on the people we know most, to get things done. If we want to be agile, engaging networks through the right trust relationships is going to win-out over engaging through the wrong ones. When we really need to react fast perhaps it is more in the speed of establishing trust between new people, new networks and new cultures where the agility is really going to come from. If one looks at the social networks of the business in contrast to the typical command and control organizational view, not only may one discover what’s really going on but you’ll also see the dynamic enterprise trust networks in action. It’s in the enterprise social networks where trust and agility live the most. Perhaps the most important task senior management has to do is to answer the question: “how can management help the business to form new trust networks adequately and quickly”. The business case to embrace mass-collaboration is starting to look pretty compelling on a number of fronts, not least of which is a step toward ‘speed of trust’ and subsequent change in personal and organizational behaviour.

A nice story in parallel of the development of the required speed of trust is the story about the underground's first escalator. This was installed at Earl's Court and went operational in October 1911. There was public fear and resistance to this new way of getting up and down and it enforced the discussion about safety and security. To show passengers how safe and easy the new escalators were, the clerk of works for the installation, 'Bumper' Harris, was employed to ride the escalator up and down each day to encourage people to use it. 'Bumper' had a wooden leg - with the idea being to show just how easy the escalator was to get on and off. Nevertheless, many passengers remained sceptical, believing they in fact knew how Bumper had got the wooden leg in the first place! Whichever side of the debate you are personally on, it seems hard to find a way to convince the other. No matter how many Bumper Harris's are on display using the new services, the evidence is used to reinforce the already held view. Nearly 100 years on, the fundamentals in bringing fundamental change about in any business or societal system remains pretty much the same.

Information security

Information must be treated holistically and must be composed out of several layers of security:

- Secure computer systems and applications
- Secure data storage
- Secure data transmission
- Provide adequate policies and processes
- Work on adequate human behaviour

SECURE COMPUTER SYSTEMS AND APPLICATIONS

It starts with the computer itself and the applications that run on it. Computer systems and applications must be adequately protected against external influences (firewalls, intrusion detection etc) and provided with the latest security patches.

SECURE DATA STORAGE

Securing data with the science of cryptography. These mathematical algorithms are used to transform originated data. The use of a cryptographic algorithm leads to such a representation of the data that is only associated with the secret key to interpret. Without the key, the encrypted data has no meaning or value. Data for secure symmetric encryption algorithms are often used as IDEA, Blowfish, Twofish, AES, Serpent, etc. Symmetrical encryption means that for this form of encryption (encoding) and decryption (decoding) the same secret key is used. Besides symmetric encryption algorithms, data security can also provided with an asymmetric encryption algorithm (RSA). This encryption method uses two different keys: one for encoding (private key) and one for decoding (public key). Asymmetric encryption algorithms require more computer resources than the symmetric algorithms. Often a combination of both encryption algorithms is applied: asymmetric encryption to exchange the secret key and symmetric encryption for encoding / decoding of data. Another form of securing data and using encryption algorithms is to split up the original data into disjointed fragments and distribute these fragments over different and unrelated servers and storages. Only with the use of a specific algorithm one can put together the originated message.

SECURE DATA TRANSMISSION

Secure communication between each computer on the Internet will be based on SSL or TLS (HTTPS connections). The current Internet browsers provide native support for this technique. SSL / TLS uses public key cryptography (asymmetric encryption) with digital certificates. The server that you connect to as a client has a digital certificate containing the Domain Name Server (DNS). A trusted authority, the Certificate Authority (CA), issues this certificate. The certificate

contains information such as name of the CA, the validity of the certificate, information about the object and of course the certified public key of the secured object. The CA signs the certificate with its private key (digital signature) and with that ensures the accuracy of the certificate data.

PROVIDE ADEQUATE POLICIES AND PROCESSES

Obviously technology is just a part of the solution. It begins with a strong vision on how security must be implemented, which policies are suitable for the data to secure and how processes support the value of secured information. Again, security policies must service the strategy of the police organization and if the policies are only getting into the way of reaching the corporate goals then policies must be redesigned.

WORK ON ADEQUATE HUMAN BEHAVIOUR

Finally people execute work, policies and processes and people make deliberately mistakes or by accident. It is quite easy to predict that incidents will occur and that a colleague is responsible for that security incident. So working with people on the value of information and the way they have to treat information is essential to make a secure environment work. That means that the force must begin with information security whenever it is hiring new employees. It also means that new employees must be screened at the right level to ensure that they have the ability to work in a sensitive environment. Furthermore the availability of information must be restricted to certain levels of authorisation, matching the employee's function and experience. It also means to train people during their employment and to share information on the subject. Finally it could mean to instate a maximum number of years to work in a specific function to minimise the risk of a cross-over.

The Jericho forum[4]

One of the concepts for alternate security is the Jericho concept brought together in the Jericho forum. The name of the Jericho Forum is derived from the destruction of the city of Jericho as expressed in the Old Testament of the Bible. Jericho was a fortified city with walls, which nevertheless was conquered by attackers.

The most succinct concept is that of deperimeterisation, the principle that information cannot be protected by the use of firewalls and DMZs[5], but that information must be protected at the level of the data elements themselves. The increasing use of the Internet as a transport mechanism, both by individuals and organizations, and the increasing integration of processes between partners in the safety value chain decrease the value of limiting the organization with 'walls'. In near future partners will not seek for a specific server on which data is stored, but will invoke a web services providing access to requested individual

data elements. The shielding of an entire server or a network segment (the traditional perimeter protection) is sparse and cannot meet the new requirements in the connected world.

The Internet is information-centric and not application-centric. REST (Representational State Transfer) is the architectural style of the Internet and Jericho an emerging security standard for it. The key goals of REST include: scalability of component interactions, generality of interfaces, independent deployment of components, intermediary components to reduce latency, enforce security and encapsulate legacy systems. With that the Internet is inherently more secure than the traditional security technologies and policies. Current, and strangely enough trusted and overrated technologies, gain access to an application through a firewall. But once behind the firewall and inside the application, a malicious user can almost do everything with all the data! In contrast the Internet only provides representations of required data, not the data itself. These representations are potentially available for any application to use. The only 4 things a user can do with data is: get it, update it, create it and delete it and security can be placed on every single information item. In this way the user can structure the required data into his own world. Therefore the Internet architecture by default enables and encourages mass-information sharing and is more secure than any other technology. By the way, that should not encourage people to put all kinds of personal data on the Internet; it must be done intelligently. If there is one call to action for corporate IT functions, it is to embrace REST and the architectural style of the Internet; ***the Internet as version 2 of the traditional corporate ICT function!***

---

[1] Reference: http://www.bourtange.nl/site/

[2] Sir Francis Bacon, Religious Meditations, Of Heresies, 1597. English author, courtier, & philosopher (1561 - 1626)

[3] H. Stiekema (2009)

[4] Bron Wikipedia

[5] DMZ (demilitarized zone) is a network segment which is implemented between the internal and external network. The external network usually is the Internet.

EPILOQUE

The unreasonable quest

This final chapter is adressed directly to you in order to create a burning platform and an immediate call for action. This book describes a vision on police work, intelligence and technology; 'Breakout! The new unreality'. Outside of work you are already living in 'information sphere'. When a police officer goes to his 'four walled factory' he puts his uniform on, uses his striped car, uses the available black wired internal network and ignites the fire wall. In fact this police officer, your colleaque, emerges himselve into a 'bubble of unreality'; it's not the only reality anymore. The information sphere, where the traditional and territorial police reality meets the virtual emerging reality on the edge of information, is the new reality in which we as police organsiations must be able to serve and protect to those who need it. This book describes a vision on policing, a vision the police being embraced by the wealth of information space and a vision to open up local police organizations around the world to connect to this information space in which 2.5 billion people communicate and collaborate worldwide. Because every day we persist in what we are doing we diminish our effectiveness to protect and to serve; unreality bites.

First of all I would like to reflect on the statement, and sub-title of this book, that the police is isolated in a 'bubble of unreality'. Where does this image come from? What are the reasons for being in such an unreal bubble? Only by understanding the process of the creation of this 'bubble' will probably lead to some answers on how to break out of this imaginary bubble. Is it a self-created bubble? What are the arguments to be in this bubble and why is it so hard to break out?

As described earlier many police organizations grew from a semi-militaristic organization to an organization that was designed to provide social security by it self. The orientation was characterised by 'them' and 'us': if 'they the public' don't follow the law than 'we the police' will re-establish the social order by using anything legitimate given to us as a tool. That organization was less part of society than it is now. It was a faced-inward organization that executed their abilities as policemen, their legitimate right to register personal data and used their legitimate right to use violence against citizens whenever necessary. This organization was also a very special legal body that was equipped with possibility of demanding private information and storing that information in some kind of database for further investigation. Indeed this type of police organization captured and stored information; it didn't share information even not amongst other police departments or colleagues.

The interaction between the police organization and society, which started early 1990th, initiated the phenomenon of sharing information and using that information in a different context. At that time the city mayor was the legal

owner for the care of public safety and demanded the police to open up and share their information with the city hall and all kinds of joint partners managing public safety. The ratio behind this harsh demand was not to open up a closed organization, but to use information in a different context and to mix that information with other sources to begin to understand underlying problems of social unrest rather than to suppress unlawful behaviour only. Pro-action towards social issues was the new orientation late 90th.
The demand on information sharing rose, but police officers were was trained, and accustomed, to keep information and information sources for themselves for very good reasons. Policemen always work on solving crimes by answering the questions: who, what, where, with what, why, how and when. Answering these questions is hard enough and they don't trust anyone outside themselves providing the right answers to these questions. Another important factor to consider is that policemen typically are the professionals who realise what intrinsic value they protect when they protect their information. In fact information in a different context could lead to different and not intended outcomes and that outcome always concerns people, whether they are victims, offenders, people accessory to a delinquency or family; it always concerns people. From the fear to do wrong to other people, policemen have the tendency to protect what they have and inherently provide the right care, context and conclusion to the criminal justice system.

This knowledge and care for information or the consequences of misinterpretation of information in combination with the new demand for openness provide hesitation to share information in general. To say nothing of the usage and sharing of information from other people not even being part of the police organization. Policemen try to do their best to be a responsible 'record' keeper and to some extend that was the most important characteristic of information technology, until the Internet appeared; from that perspective the Internet is a scary place to be.

The new demand for openness exposes other organizational characteristics, which could easily lead to the idea of an imaginary bubble surrounding the police. Next to the already mentioned individual training to keep their records impeccable, a traditional concept of reality and the slow tracking of social developments are the other seeds to bloom hesitation and reluctance to share information. The whole information environment was in balance somewhere between the early 70th and the late 90th. A solid balance was then found between the organizational goals and the individual police officer and between the organizational goals and public prosecution. This balance was challenged early 21st century by the new opportunities of information technologies and the short technology cycles.

As a consequence the self-created bubble wasn't really self-created, but originated from the care for society and the care for people living in it. It also originated from a care for its own police image as trustworthy partner to 'protect and to serve'. Clearly the cause of the imaginary bubble is hidden in the culture of the organization and in the principles the police lives by. The increased demand for getting professional signals and advises on social security issues out of the police organization, and into the collaborative security network, is one of the main reasons the police has to cope with the new digital world. The best thing to do is to explore this new world internally and in a broad social debate; the worst to do is to nourish the culture of isolation.

In that respect Internet as 'version two' of corporate information and communication technology and Internet as a new organizing principle for the future police organizations, is a challenging if not *'an unreasonable quest'*. Being unreasonable seems to be reasonable in a time where there is a lot of doubt around the way society trusts policing, where there is a lot of fear the way society develops as one looks closely to 'pearls in policing' and the increased necessity to enforce protecting and serving our citizens. I am quite sure that if we launch this unreasonable quest as being the corporate vision, all kinds of people, institutes and administrations will join and line up to defeat this quest; try to stop it. Yet I have no hesitance or doubt to propose as such and neither should you.

To follow through on this unreasonable quest your organization needs a few things to put in place:

- shared interest. Regroup the organization, redefine existing paradigms about communication, collaboration, information technology and so on and build a sustainable business to protect and serve better than ever before with more efficiency.
- leverage. The down side of not doing anything in the new era or changing too slow is a growing chance of diminished legitimacy. Budgetary con straints will then affect the organization even more.
- corporate communication. It's important that the organization really talks with one voice, stating one message leading towards one general set of goals.
- belief structure. Police management must belief in this chance to happen and consistently manage the organization into the 21st century

In order to get to the starting point we must start debating on the paradigm shift at hand and embrace the transformation with a meaningful context. Stop debating about wrong or right and lead the organization towards a collaborative environment where citizen's security is served best. Lead your organization to grow a mature organization with a network structure and a strong information

centric fundament with supporting technology. Develop an organization that is sparkling for young employees, partners, scientists and volunteers and all kinds of partners we don't know yet. Lead your organization in building a police 'tribe' into the heart of society again. Finally lead your organization into the 21st century; with imagination!!

To enforce the sense of urgency even more, you can join the (inter)national police community on www.ipep.info or www.politie20.nl. Live on the Internet, live in information space and live on the white wire!! Meet interesting minds, get new organizing principles and a community that can and will support you in your work for society.

I have tried to show you that there is a wealth of opportunities in this new connected world but also a dark unknown world that we have to discover. For the sake of societal promises I would like to ask you urgently to replace the word 'opportunity' with 'obligation'. The obligation of leading this change, the obligation to change for future colleagues and the obligation to the citizens you protect and serve so well. Do not make your police organization part of a network of police organizations, but make is part of a much broader and valuable societal network. One person can do it. You can do it.

Thanks for joining this ride

Huub Stiekema

REFERENCES

Literature

Alles onder controle,
A.M. Arnbak, July 2009

Atos Origin, Web 2.0 and Policing today in the Netherlands,
C. Bate and H. Stiekema, September 2009

British Society of Criminology (BSC), Policing diversity in the digital age,
David, S. Wall and M. Williams, December 2009

Cap Gemini Technovision 2012,
O. Freese, R. Tolido, T. Nachtwey, P. Hessler, October 2007

CIO Counsil Web 2.0 security working group, Guidelines for secure use of social media by federal departments and agencies version 1.0,
September 2009

Crime Analysis for problem solvers,
R. V. Clarke, J. E. Eck, August 2005

Data voor Daadkracht,
Rapport van de adviescommissie informatiestromen veiligheid, 2007

Global CIO Survey 2008, The role of the IT function in business innovation, 2008 Cap Gemini

Global trends 2025, A transformed world,
US Government printing ofice, novermber 2008

Informatierijk en toch kennisarm,
Lectorale rede van dr. Ir. M. Den Hengst-Bruggeling, maart 2010

Intermediair, Bedrijfsstrategie en informatiestrategie vallen steeds meer samen,
H. Hilgenberg, December 2000

Lost in translation,
N. Green, C. Bate, November 2007

Netwerkend werken en Intelligent opsporen,
prof. Dr. A. Roobeek en M. Van der Helm MSc, October 2009

Operational Intelligence
Richard Veryard, Director of the Next Practice Research Initiative

Police CIO forum, International police agencies,
Cap Gemini, Annual meetings

Politie in ontwikkeling,
B. Welten, May 2005

Reframing the future, Policing in a modern networked environment,
A. H. Seng, Singapore, 2008

The McKinsey Quartely, Eight business technology trends to watch,
December 2007

The new norm,
C. Bate, October 2009

The next wave of innovation in eGovernment,
Dan Rasmus

The Open Group, Identity management,
July 2002

The rise of the network society,
Manuel Castells, 2010

Trendsignalement 2009,
Centrum voor criminaliteitsprecventie en veiligheid, 2009

Tribes,
Seth Godin, 2008

Trust in Mashups,
Cap Gemini, 2008

Vooruitzien is regeren,
prof. Dr. Ir. A.J. Berkhout, prof. dr. W.J. de Ridder, 2003
Webcam toezicht, Digitaal achter de geraniums,
L.J.A. Engbersen, July 2008

Wenkend Perspectief, strategische visie op politieel informatiemanagement en technologie
2006 – 2010, H. Schönfeld, H. Stiekema, december 2005

Situating the police in cyberspace,
David Wall, Informa world

Trendrapportage Veiligheidshuis Eindhoven,
Marieke van Hoof, 25 april 2007