Resolution
of the European Confederation of Independent Trade Unions (CESI)

Use of modern technology in the public security sector

Rapporteur: Stéphanie Larosa
Brussels, 12 July 2013

Modern technology, including information and communication technology (ICT), have generated renewed economic growth at the same time as reshaping the working methods of most employees.

These new technological tools often simplify tasks and, in the public security and safety sector, they permit the faster resolution of inquiries, allow crisis management, the fight against cybercrime, and the provision of compelling evidence in the justice sector, with the aim of protecting citizens and states against all forms of aggression, including terrorism.

Currently, more than ever before, this technology is at the heart of discussions on a European level, as can be seen in the debates on data protection or cybercrime. In the case of cybercrime, it is defined as "one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technology offer in order to commit a diverse range of criminal activities". Cybercrime allows criminals to commit already existing crimes much more easily, such as money laundering, child pornography, incitement to hatred and terrorism, for instance. Moreover, it has also led to the creation of new types of specific offenses linked to new information and communication technology, such as the hijacking of personal and banking data.

1 Interpol’s definition of cybercrime
Therefore, the public security and safety sector is particularly concerned by these developments. Crime has never stopped at borders, but now, it has become even more serious due to criminals’ use of IT tools.

The responsiveness of law enforcement agencies and governments is essential in this constantly changing environment. Criminals’ use of increasingly efficient technology means that public authorities must adapt to the circumstances.

Thus, it is fundamental that the Member States should join forces to face this malicious use of modern technology. Although there are many examples of such efforts, CESI is of the opinion that a more ambitious policy could be implemented.

In this view, it is fundamental that the focus be on the training and equipment available to public security agents when legislative texts are written up on security issues linked to the use of modern technology, whether on a European level or on a national level.

In the same vein, the objective of the use of modern technology by public security services in Member States should be the improved performance and better working conditions of the concerned employee(s). They should not aim to reduce the means allocated to ensuring the security of citizens and agents, namely in the context of their duties. Particularly, the use and ability to use modern technology should offer the possibility of a better organisation of one’s tasks, by permitting access to information practically instantaneously, along with the exchange and sharing of data amongst all public security actors, both on a national and on a European level.

Finally, the dissemination of new media has also led to new risks appearing, such as cyber-bullying and cyber-mobbing. These risks are particularly high for law enforcement employees, and specific attention will have to be paid to ensure the security of acting agents and prevent all outside pressure that could have a negative impact on their profession.

The Security Trade Council, a body of the European Confederation of Independent Trade Unions, is composed of active professionals from national and local police forces in the Member States, as well as of civil security forces and customs personnel. This Trade Council held a meeting on 29 April 2013 which allowed professionals from the field to express their opinions on the use of modern technology in the public security sector.
RESOLUTION OF THE EUROPEAN CONFEDERATION OF INDEPENDENT TRADE UNIONS

regarding the use of modern technology in the public security sector

THE EUROPEAN CONFEDERATION OF INDEPENDENT TRADE UNIONS,

having regard to the Treaty on the Functioning of the European Union, particularly Title V, The area of freedom, security and justice, its articles 152 and 153;

having regard to the Charter of Fundamental Rights of the European Union, particularly articles 8 and 31;

having regard to the Stockholm Programme, an open and secure Europe serving and protecting citizens;


having regard to the Cybersecurity Strategy of the European Union, an open, safe and secure cyberspace JOIN (2013)1 final;

having regard to the Proposal for a Directive on attacks against information systems repealing Council Framework Decision 2005/222/JHA;

following a consultation of the members of the Security Trade Council;

***

highlights the transnational nature of delinquent and criminal acts, namely when they make use of modern technology.

welcomes the publication of a first European cybersecurity strategy.

supports all initiatives that contribute towards an improved fight against cybercrime and towards the improvement of police and judiciary cooperation in such matters.

invites, however, European political decision-makers, i.e., the Commission, the Council and the Parliament, to follow a more wilful cooperation policy in this area.

calls upon the Member States to grant themselves the necessary means to establish a European policy to fight a form of crime that does not stop at borders and that is becoming increasingly digital.
demands that employees of public security forces receive adequate training to enable them to master modern technology and improve their ability to respond to new forms of crime.

demands adequate equipment to improve the performance of agents. It is fundamental to invest in the most modern technology available, in order to prevent the appearance of a gap between criminals and law enforcement.

opposes a use of modern technology that would lead to a reduction in staff numbers. Modern technology is a tool that can improve the performance and working conditions of agents.

condemns the use of modern technology that would act as a disguised tool to spy on police agents in action and turn them into suspects. This type of attitude would simply give criminals additional excuses and make them less accountable for the offenses they have committed.

warns political decision-makers on the birth of new risks for law enforcement employees, namely cyber-bullying and cyber-mobbing.

believes that geolocalisation technology must first and foremost be used to protect citizens and acting agents, not to control agents and their trade union representatives. It is proposed that this type of technology only be used during intervention periods.

is in favour of the maintenance of the State’s sovereign missions for European public security forces (police, civil security,…). The lack of technical knowledge could be remedied by improved cooperation with the private sector, but this does not mean that the public sector should lose its autonomy by losing qualified personnel, for instance. The use of private actors shall be undertaken for specifically-defined missions, within the framework of national or European calls for proposals.

It is fundamental and essential that the countries of the European Union organise themselves in a structural and concerted manner to fight this new form of crime and protect and preserve the sovereignty of European police force missions.

Thus, today more than ever, it is crucial that we know how to organise ourselves on a European level and act jointly to protect the citizens from an anonymous and borderless form of crime.