FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Collaborative Project

SURVEILLE Deliverable 3.4: Design of a research methodology for assessing the effectiveness of selected surveillance systems in delivering improved security

Due date of deliverable: 30.09.2013

Actual submission date: 30.09.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP03 Dr. Coen van Gulijk

Author(s): Coen van Gulijk, Simone Sillem, Michelle Cayford (TU Delft)

SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

§ 0 Executive summary

This report deals with the assessment of effectiveness and efficiency of surveillance technologies. Unfortunately, there is little consensus and clarity about these types of assessment for surveillance technologies, nor is there a clear definition of the terms in the open literature. Therefore, this report begins by defining effective and efficient for surveillance technologies for use in the SURVEILLE project. The definitions are as follows:

Effective surveillance technology has the technical capacity to deliver the intended security goals, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome.

Efficient surveillance technology delivers the intended security goals with low use of resources in terms of cost, time and/or physical and mental efforts.

The open-source literature also lacks clear frameworks or methods for effectiveness and efficiency assessment of surveillance technology. Therefore a number of frameworks or methods were gathered that may be used to construct sensible assessment tools and could form the basis for ex-post analysis of surveillance technologies. They are:

- the value analysis process by Roland,
- ISO 31.000: risk management,
- FEMA's point-scoring method for assessing terrorist threats to buildings,
- the CDC model for ex-ante evaluation of surveillance systems for infectious diseases, and
- a quantitative operations analysis that was designed by RAND for the ex-ante evaluation of the efficiency and effectiveness of RPAs.

The envisaged (or rather possible) use of these methods is described using the MerPol crime-investigation scenario where a number of surveillance technologies are indicated. This study shows that a number of prerequisites are necessary for effectiveness and efficiency analysis. First, the goals for the surveillance technology in the given context have to be specified precisely and concisely. Without goal setting, any evaluation of effectiveness or efficiency becomes vague in the sense that retrospective analysis becomes open to speculation about the intentions of the users. Second, an evaluation of actual use is required; either for each individual use of surveillance technology or for surveillance technology groups in specific contexts (such as a serious crime investigation). Third, the earlier experiences and evaluations have to feed back into future uses of the technology; written reports (preferably with standardized layout and topics) are invaluable for this step. These steps can be captured in structured frameworks that may be developed from ISO

31.000, the FEMA method (with semi-quantitative scores) or the value assessment process.

The analysis in this report shows that the semi-quantitative crime risk scoring method of the FEMA method is best suited for further development in the SURVEILLE project. With this framework, effectiveness/efficiency research findings can easily be retained in the scoring system, the framework is relatively easily interpreted and the framework is flexible enough for discussion when a point-scoring exercise is performed.

Further research in work package 3 of SURVEILLE will focus on the development of a point scoring method of which the FEMA framework is an example and the decision matrix in SURVEILLE deliverable D2.6 is the template.

Contents

§ 1 Introduction

§ 1.1 Addressing effective and efficient surveillance

The title of this deliverable suggests that there is a significant body of knowledge concerning the effectiveness of surveillance technology. This, however, is not the case. While surveillance technology has developed rapidly over the past decade and its application continues to rapidly spread, there has not been a parallel development of evaluating the effectiveness of this technology. This is even the case with CCTV, which is perhaps the best-known technology when it comes to surveillance. CCTV has been around for a while and a significant body of experience was developed for it. Much of that discussion is covered in deliverable D2.3 of the SURVEILLE project called 'Paper by local authorities end-users.' That paper shows that end-users tend to judge the success of CCTV in a more positive light than researchers do and that the outcome, in security-gain, varies a lot between individual studies.

When we started research on the effectiveness and efficiency of surveillance technology the first thing that was apparent is that there is no consensus on what efficiency and effectiveness are in the surveillance context. Crime researchers study the effects on crime (e.g. Gill & Spriggs[1]); technology developers' focus on improved technical capabilities (e.g. Rios-Cabarera et al.[2]); economic evaluators focus on large-scale crime-control programmes (see future deliverable D3.5 'cost model'). However, an effectiveness assessment of a surveillance technology deployed in a certain context is absent. Even a useful definition is absent. Therefore §2 of this report discusses the definitions of 'effective' and 'efficient' in relation to surveillance technology.

A considerable effort was spent in finding systematic efficiency assessment methods that are applicable to surveillance technology. The *scientific* literature is virtually void of clear descriptions of surveillance evaluations (or structured evaluation methods) when it comes to efficiency or delivery. We found the most relevant to be in the domain of safety and risk control but we can also learn from surveillance systems for infectious diseases. Note that this is mostly 'grey' literature. That is to say, the documents are not peer-reviewed works of research; they are reports from governmental agencies or NGOs that lack rigid peer reviews. Several methods for effectiveness assessment are treated in §3.

---

[1] Gill M. & Spriggs A. *Assessing the Impact of CCTV*. Home Office Research Study No. 292.

[2] Rios-Caberera R, Tuytelaars T. & Van Gool L. "Efficient multi-camera vehicle detection, tracking and identification in a tunnel surveillance application," *Computer vision and image understanding* 116: 742, 2012.

§4 reports the application of five assessment methods to the MerPol scenario developed in SURVEILLE. This scenario describes the use of surveillance technologies and the problems that have to be solved with them. The assessment methods are applied to these problems. It is important to mention here that the evaluation techniques described in §3 would have to be adapted for actual application in the field. For the sake of demonstration, we show how these methods would work in the context of this scenario. This provides insight into the usefulness of evaluation methods and relevant parameters for the development of a new research methodology.

§5 discusses the results and §6 draws conclusions.

§ 1.2 Position of the report in SURVEILLE

This report is entitled 'Research methodology for assessing the effectiveness of selected surveillance systems in delivering improved security.' It is a deliverable in work package 3 of the SURVEILLE project. It contributes to the following objectives of work package 3:

O3.1 To assess the benefits and costs of surveillance technology. (By 'benefits' we mean the delivery of improved security; by 'costs' economic costs, negative public perceptions, negative effects on behaviour, and infringement of fundamental rights.) (project objective O2)

O3.2 To produce proposals for improving the effectiveness of security surveillance, while taking fully into account perceptions, economic costs, legal limitations and ethical issues.

With regard to O3.1 this report focuses on the delivery of improved security; where the delivery is an aspect of effective surveillance. With regard to O3.2 it focuses on improving effectiveness by defining the term in the surveillance context and assessing systematic evaluation frameworks.

Note that other parts of these objectives are met in deliverables that are produced almost simultaneously with this report. They are:

D3.2: European level study on perceptions, including an overview of effects and side effects of surveillance and their perceived effectiveness

D3.3: System effectiveness, efficiency and satisfaction assessment

D3.3b: Report on system effectiveness, efficiency and satisfaction assessment

D3.5: Cost model for surveillance techniques

These reports (and this work) focus on collecting prior knowledge in different fields (perception, financial cost, satisfaction, efficiency and effectiveness). The authors suggest reading those reports alongside this report because they demonstrate how difficult technology assessment is.

Further developments for surveillance technology assessment require decisions for the design of the research apparatus that have to be based on these reports and on a discussion with all SURVEILLE partners.

§ 2 Effective and efficient

§ 2.1 Background

Though the technical scientific literature is full of new developments in technical capabilities that could contribute to capturing terrorists or criminals involved in serious crime, the question of whether these technologies are effective or efficient in a broader societal context is never discussed there. In technical reports the term 'efficient' is used to demonstrate that a new technological development works faster, is simpler, or consumes less energy than the prior technical development, but the question of whether it delivers improved security to society in a cost-effective way remains mostly absent. This is a handicap for the SURVEILLE project where we actually ask ourselves which surveillance technologies deliver effective and efficient service to society in its struggle to fight serious crime and terrorism.

The problem was already described in deliverable D2.3 of SURVEILLE entitled 'Paper by local authorities end-users' where the authors ask themselves (regarding surveillance technology): Does it work? That report claims that the feedback from municipal authorities connected to the EFUS panel (over 250 municipalities in Europe) exchange positive feedback amongst themselves. Success stories include reduction of anti-social behaviour, disappearances of drug scenes, disappearance of prostitution, offenders caught in the act, and successful crime investigations based on CCTV footage. Independent researchers, however, are less certain. The report cites a number of official research efforts (focused on CCTV) that mostly show mixed results on crime: some positive, some negative and some with no effect at all. This ambiguity is not very helpful for the discussion in this report where the effectiveness and efficiency of surveillance technologies are discussed. But the problem runs deeper: clear definitions of 'effective' and 'efficient' are lacking when it comes to surveillance technology.

The first question that arises in developing a methodology for assessing the effectiveness and efficiency of surveillance technology, is what do we mean when we say 'effective' or 'efficient'? In examining studies and reports on surveillance technology produced by governments and third parties (REFS), as well as current discussions in the SURVEILLE project, two things quickly become apparent:

1) The *efficiency* of the surveillance system is discussed alongside its effectiveness, and the two words are often used interchangeably. Therefore, 'efficient' must be defined and included along with 'effective' in the assessment of selected surveillance technology.

2) There is no laid-out definition of 'effective' or 'efficient' when speaking of surveillance systems. In one, specific RAND report analysing remotely piloted aircraft, 'operational effectiveness' was defined as follows: "The operational

effectiveness of a system can be defined as the degree to which it improves the warfighter's level of success in a given set of missions or enlarges the range of conditions under which the warfighter is likely to be successful in those missions."[3] In general, however, 'effective' and 'efficient' are used in discussions and evaluations to describe how a system or technology should operate, but without explaining what this means (i.e. "the system should function effectively").

§ 2.2 Defining effective surveillance technology

We could assume that the authors of the RAND report are just using the terms as defined in the dictionary, but even this would need some adaptation to the realm of surveillance. Without explicit definition, the door is also left open to interpretation, leading one person to say the technology is effective, while another says it is not, each one having a different idea of what 'effective' is.

Despite that, there is a general consensus that for surveillance equipment to be effective it must work as desired, that is, perform as it is intended to. There are at least three layers of what this means. The first layer addresses the question whether the equipment is performing on a technical level. CCTV, for example, is made to video a particular area. Likewise, armed drones are designed to locate and launch an armed missile at an intended target. If the equipment is successfully performing these tasks it could be called effective. Often the term 'reliable' is used to describe this level of performance. This type of effectiveness (or reliability) could be captured by numbers: for instance, the CCTV is operational for 95% of the time and 5% of the time it is in repair; or, a drone fails to video a suspect 15% of the time because commands cannot be transmitted to it due to weather conditions.

The second level is the technical success ratio: given that a system is not failing, how often does it achieve the technical goal? For CCTV this means that a crime, such as theft, is actually recorded. Again, numbers can be used to describe the effectiveness, in which case it should be viewed as a success ratio. Out of 100 crimes that take place in front of the camera, how many are recorded by it so that the crime could, in principle, be detected.

The third layer, describing the intended effect of the government and the expectation by the public at large, in deploying this equipment, goes beyond the technical features. The desired and expected outcome of installing CCTV in a city is that crime would be controlled and prevented and the crime rates reduced. The U.S. government, in employing drones in Afghanistan, has argued that they are effective at eliminating al-Qaida while limiting civilian casualties.[4] The desired outcome is to eliminate terrorists with minimal civilian casualties. Here, the judgment of

[3] RAND, *Methodologies for Analyzing Remotely Piloted Aircraft in Future Roles and Missions*, 2012, p.4.

[4] Matarrese, Andy, "U.S. official defends drone strikes as legal, effective," *UPI.com*, 1 May 2012. Web. 6 March 2013.

effectiveness is intermixed with political, ethical and other forms of opinionated judgment.

It is clear that in order for the effectiveness of surveillance technology to be measured these three levels need to be distinguished and aligned. For that to work, the goal for which the surveillance technology is employed must be clearly stated. Is CCTV being implemented to prevent crime or to aid in successfully prosecuting criminal acts it captures? If the goal is to reduce crime rates does this mean all crime rates, or specific types of crime? Discussion abounds on whether or not CCTV is effective, and (arguably) the conflicting views and results of studies could be attributed to this problem of the goal of the installation of CCTV not being clearly stated (or its purpose being too broad). Only when a clear goal is stated unambiguously and precisely is a coherent discussion about effectiveness possible. Once clear goals are stated, effectiveness becomes a meaningful term. In this work we propose a definition that is derived from a generic statement for effectiveness in ISO 9241: effectiveness is the accuracy and completeness of user goal achievement. For surveillance technology we propose:

Effective surveillance technology:

Effective surveillance technology has the technical capacity to deliver the intended security goals, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome.

§ 2.3 Defining efficient surveillance technology

Like effective, efficient is only a meaningful term after a goal or goals are set. So the need for unambiguous and precise goals is the same as for effective.

Whereas effectiveness relates to the rate of success of achieving a goal only, the efficiency takes the magnitude of the task into consideration. That is to say, that a large or difficult goal (e.g. the eradication of crime in a major city) justifies considerable efforts; a simple goal (e.g. preventing jaywalking near a zebra-crossing) does not justify large efforts. In that sense, efficiency is scalable with the magnitude of the goals.

Assuming that clear goals are set, efficiency combines a number of factors. It is, like effectiveness, a multi-faceted problem, including but not limited to: costs, labour, time and simplicity of use.

Unfortunately, the efficiency of surveillance technologies is even less well documented than the effectiveness of surveillance technologies, which gives us

much freedom in defining the term. Again, the definition for surveillance technology is derived from the definition of efficiency from ISO 9421 where a process is said to be efficient when a minimum of resources is spent in order to ensure accurate and complete achievement of the goals. This is translated to surveillance technology as follows:

Efficient surveillance technology

Efficient surveillance technology delivers the intended security goals with low use of resources in terms of cost, time and/or physical and mental efforts.

This definition, and the definition for effective surveillance technology will be used throughout this report.

§3. Effectiveness and efficiency assessment for surveillance technology

Unfortunately, there are no clear guidelines for the assessment of effectiveness or efficiency of surveillance technology. This chapter describes frameworks and methods that are used in other risk areas. This provides the SURVEILE project with a number of frameworks that can be used as a basis for the development of a research methodology for the assessment of effectiveness and efficiency for surveillance technology.

Five methods are treated in this chapter *viz.* the value analysis process by Roland, ISO 31.000: risk management, FEMA's point-scoring method for assessing terrorist threats to buildings, the CDC model for the ex-ante evaluation of surveillance systems for infectious diseases and the quantitative analysis that was designed by RAND for the ex-ante evaluation of the efficiency and effectiveness of RPAs.

§3.1 Roland's value analysis process

A fairly straightforward framework for the evaluation of risk controls is given in a textbook for system safety engineering by Roland.[5] Roland produced this textbook for risk and safety education in 1990. Amongst basic elements of safety management, statistical safety analysis and system analysis, it treats decision analysis for safety systems. The element that is useful in this work is called the 'value analysis process', depicted in figure 1.

[5] Roland HE & Moriarty B. *System safety engineering and management* 2nd ed., John Wiley & Sons, New York, 1990.

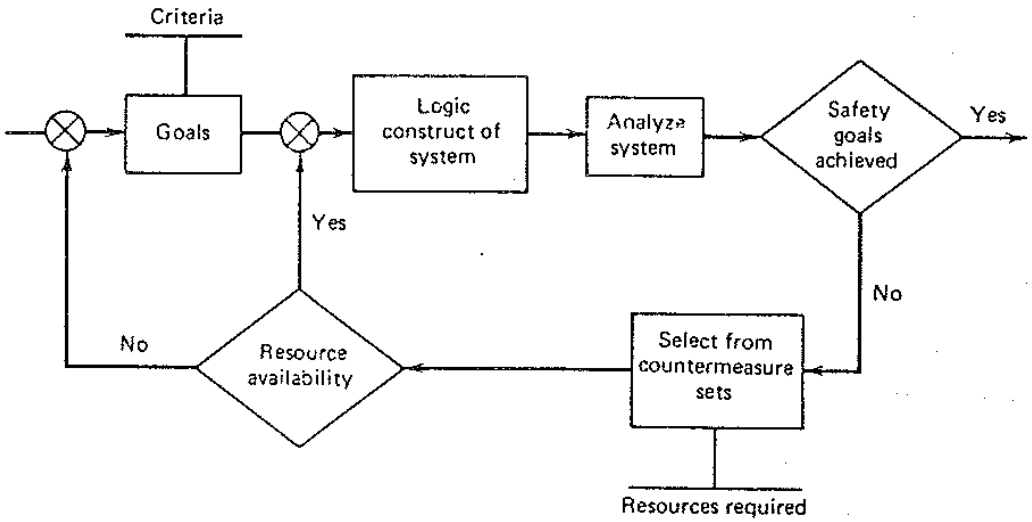

Figure 1: the value analysis process[5]

Purpose of the model

The value analysis process refers to an interactive decision process that connects the elements of the decision process and specifically includes achieving safety goals. The process focuses on safety goals and the level of success that can be attained within the constraints of achieving the goals and the resources available.

How does it work?

The process starts by setting goals that are relevant to the safety problem. These goals are achieved through specific countermeasures, technologies or work processes. The second step is to develop an analytic model of the system in which the goals and countermeasures have to be incorporated. Once an analytic model is developed, the analysis may be performed. Usually, this includes historic data; that is to say, some results from earlier experiences are fed back into the decision-making process. This analysis demonstrates how well the goals are achieved, i.e. how effective the technology is. That analysis encompasses an assessment of the effectiveness and efficiency. When the outcome is satisfactory, the goals or instruments to achieve those goals do not have to be changed. Otherwise changes have to be considered in a new set of countermeasures, technologies or methods. These changes also force a review of the resources and goals. The complete process forces a cyclic review process of safety goals, countermeasures and the success rate of the system.

Information needed for the evaluation of effectiveness / efficiency

In its current state, this process cannot be used to test effectiveness and efficiency. A lot of information is necessary for the evaluation of effectiveness and efficiency. Firstly, specific and clear goals for the risk goal are required, in this case, the level of achievement required from surveillance technology. Secondly, descriptions of the technologies and their contribution to successful surveillance are required. Based on that information an analytic model has to be developed. Note that the model does not have to be a complex computational model (as suggested by the RAND method); rather the analytic model has to provide a systematic process for evaluating technology. At this point, such a model is not available for surveillance technology.

Advantages / disadvantages

The advantage of this process is that it introduces a cyclic review process. The effectiveness or efficiency is evaluated periodically or every time that the technology is used. Such cyclic processes demand continuous attention for effectiveness and efficiency. In addition, cyclic review processes enable trend analysis over a prolonged period of time; however, for trend analysis record keeping is important too.

The most important disadvantage with this method is that it is abstract; that is to say, it offers very little handles for implementation in practice. Also, it demands the development of an analytic model. It is not clear what this model should look like or what the requirements are for that analytic model. In that sense, this process is underspecified and would require further development for use in SURVEILLE.

Usefulness for this deliverable

Although the value analysis process is underspecified, the introduction of cyclic evaluation processes for efficiency and efficiency is, nonetheless, a sensible step. It allows for periodic review and trend analysis, which help in deciding which surveillance technology is efficient for which task.

Methodology for assessing effectiveness of surveillance technology

No method is described for assessing the effectiveness of surveillance technology. The process simply states that goals must be set, countermeasures (surveillance technologies) have to be selected and a dedicated evaluation process should be used to assess effectiveness, but it does not describe how to do that.

§3.2 ISO 31.000

The Risk Management system as described in ISO 31.000 describes a number of principles that need to be satisfied to make risk management effective.[6] It recommends how a framework for managing risk should be developed, implemented and continuously improved. This framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. Figure 2 shows the risk management cycle as it is used in ISO 31.000.

Note that surveillance technologies are instruments that may be used to support two processes in the ISO framework: risk identification and risk treatment. When surveillance technology is used for risk identification it is employed to find new criminal pathways, new modus operandi or to identify individuals previously unknown in criminal networks. An example of this is when a crime analyst is uncovering new drug-trafficking routes. When surveillance technologies are used for this purpose the knowledge position of the police or other crime fighting agents is improved. The technologies may also be instruments for risk treatment, that is to say, to control known crime risks and to influence those risks. The prime example is luggage screening in airports where the detection of an illegal weapon such as a gun, immediately leads to a response by security personnel and/or law enforcers.

[6] NEN-ISO 31.000 *Risk Management – Principles and guidelines* (ISO 31000: 2009, IDT)

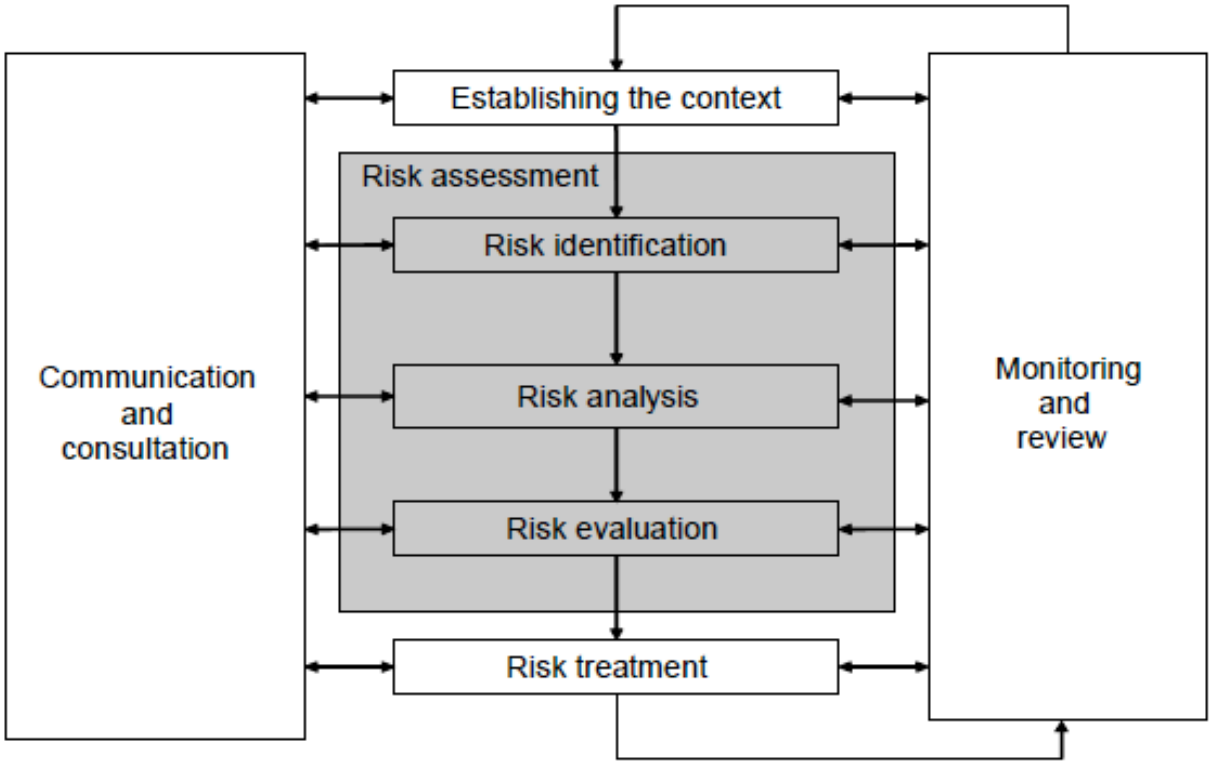

Figure 2: ISO 31.000 the risk management cycle[6]

Purpose of the model

Primarily, the ISO 31.000 standard provides guidance on the selection and application of systematic techniques for risk assessment. The application area of this standard is very broad. The document states that the framework is useful for organizations of all types and sizes that face a range of risks that may affect the achievement of their objectives. The objectives may vary from strategic initiatives to operations, processes and projects. The risks themselves may be described in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts. Note that the standard provides guidance rather than operation standards or auditable rules. The document specifically mentions that methods that have not reached a satisfactory level of professional consensus are not included. The emphasis is on the design of logical and systematic methods for:

- communicating and consulting throughout this process;

- establishing the context for identifying, analysing, evaluating, and treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the results appropriately.

How does it work?

The methods in the document are dedicated to answer fundamental risk management questions:

- What can happen and why?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?
- Is the level of risk tolerable or acceptable and does it require further treatment?

The mechanism for answering these questions is a step-by-step analysis program that addresses the five 'core elements' of risk assessment (as in figure 2): communication and consultation, establishing the context, risk assessment, risk treatment, and monitoring and review. Each of these steps is explained in the standard and suggestions are made for techniques or methods to address these core elements. Thirty-one risk methods are briefly described as candidates for risk analysis including: check lists, structured and semi-structured interviews, root-cause analysis (for incidents), HAZOP, fault-tree analysis, bow-tie analysis, Markov analysis and cost-benefit analysis or CBA. Some of these techniques (bow-tie; CBA) are mentioned in other deliverables for the SURVEILLE project.

The structured analysis leads to documentation that describes the risk problem. The ISO standard says the following about documentation: "The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear. The extent of the report will depend on the objectives and scope of the assessment. Except for very simple assessments, the documentation can include:

- objectives and scope;

- description of relevant parts of the system and their functions;
- a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed;
- risk criteria applied and their justification;
- limitations, assumptions and justification of hypotheses;
- assessment methodology;
- risk identification results;
- data, assumptions and their sources and validation;
- risk analysis results and their evaluation;
- sensitivity and uncertainty analysis;
- critical assumptions and other factors which need to be monitored;
- discussion of results;
- conclusions and recommendations;
- references."[7]

This documentation should form the basis in decision-making processes about risk control and provide the blueprint for further steps in risk control.

Information needed for the evaluation of effectiveness / efficiency

ISO 31.000 is not specifically dedicated toward the evaluation of effectiveness or efficiency; it is primarily aimed at the construction of a risk control system. The evaluation of effectiveness and efficiency is a subsidiary task in the risk management system: monitoring and review. Monitoring and review encompasses a number of tasks: checks whether key assumptions about risks (and the analyses themselves) are still valid; monitoring whether expected results are being achieved; and whether the risk treatments are effective. ISO 31.000 states that the effectiveness of a risk treatment should be monitored, but it is neither mentioned how this should be done nor are techniques or methods described.

The information requirement for this technique varies with the level of ambition for risk control and the complexity of the risk problem. If it is applied to surveillance

[7] NEN-ISO 31.000 *Risk Management – Principles and guidelines* (ISO 31000: 2009, IDT), p.16.

technology in a specific environment, it is sensible to construct a risk assessment document as indicated by ISO 31.000. This requires information about the objectives of the surveillance application; a description of the technology and application area; a description of the context (juridical, technical, organizational); and data that may be necessary for a chosen risk analysis technique. When the risk analysis technique is a relatively simple one (e.g. a bow-tie analysis), the data-requirement may not be very demanding. When the risk analysis technique is technically challenging (say, a fault-tree analysis) the data requirement may be formidable. ISO 31.000 does not provide guidelines for surveillance technologies; that would have to be developed for this specific group of risk measures. Once such an exercise has taken place it may be much easier to perform an assessment rather than starting from scratch every time.

Advantages / disadvantages

A distinct advantage of using this framework is that it is a globally accepted method for dealing with risk problems. ISO 31.000 provides a framework for risk control, a relatively straightforward stepwise working procedure, and gives suggestions for risk estimation and control methods. Note that the global acceptance of this framework is a relatively new development in the design of risk management cycles. The basic concept of a risk framework matured during or directly after WWII[8]. And various risk management cycles were developed for dedicated industries such as air transport[9], the chemical industry[10] or as a generic risk management model[11]. The risk management cycle has been tried and tested over the years and there are many experts around the world that know how to work with it. A second advantage is that the method is, in principle, a generic one. That enables the development of a dedicated risk management system for surveillance systems. In this case, additional steps or phases can be introduced in the risk management cycle and specific instructions about surveillance can be developed for use in decision-making processes.

A distinct disadvantage is that the method stems from industry practices rather than legal practices. The legal framework is not considered explicitly but is implicitly part of the 'context' of the framework. For surveillance, which is strongly regulated through legislation, it may be less suitable.

Usefulness for this deliverable

[8] Heinrich H. *Industrial accident prevention*. 3rd ed. McGraw Hill Book Company New York, Toronto & London, 1950.
[9] Safety Management Manual. ICAO document 9859 AN/490, 2006.
[10] Cameron I, Raman, R. *Process systems risk management*, Elsevier academic press, Amsterdam, 2005.
[11] Ale B. *Risk, an introduction*, Routledge, London, 2009.

The ISO 31.000 demonstrates that practical frameworks exist to control dangers in the risk/safety/security domain. These methods are rarely treated in legal disciplines but are used frequently in operational safety, risk and security control, especially when it comes to high-risk industries. The framework demands monitoring the effectiveness of risk control measures, which means that incidents need to be registered. The incident reports are periodically analysed to assess the effectiveness of measures and so introduce a continuous assessment for effectiveness. That mechanism, together with registration systems, is useful for the assessment of the effectiveness and efficiency of surveillance systems. The second useful element is that a risk analysis is required. A risk analysis forces an analyst (and ultimately a decision maker) to consider the magnitude of the risks and what to expect from one or more control measures. Also, it provides a starting point for the desired effect of the control measure (e.g. a CCTV camera). The third useful element is that a quite detailed document is required that addresses relevant elements for the understanding of the risk problem. For the selection and/or use of surveillance technologies such a document would be useful as a reference for decision makers, lawyers, and operational staff so that they understand the complications associated with a technology in a specific surveillance situation.

§3.3 FEMA

Another example of a methodology developed for a particular case is the U.S. Federal Emergency Management Agency's (FEMA) risk assessment for terrorist attacks against buildings.[12] This model also generally follows the risk management cycle: identification, quantitative analysis (there are elements of qualitative analysis as well, but for the most part it is quantitative), decision, as well as reduction elements.

Purpose of the model

FEMA developed this risk assessment model to provide a clear and comprehensible methodology to do a risk assessment. The risk in this case is a terrorist attack on a building. The target groups of FEMA's guide for risk assessment are architects, engineers, building owners / managers and government officials. The guide outlines methods that can be used to identify critical assets, determine the actual threats to those assets and assess the vulnerabilities that are associated with those threats. This can then be followed by a risk-based decision on how to mitigate these risks.

How does it work?

The FEMA Guide generally follows the risk management cycle. The five steps that are considered in figure 3 are part of the risk management cycle. How they fit within the risk management cycle is seen below:

- Establishing the context
- Risk assessment
    - Risk identification
        - Threat assessment (Step 1)
        - Identify the value of the building's assets (Step 2)
        - Vulnerability assessment (Step 3)
    - Risk analysis
        - Risk assessment (Step 4)
    - Risk evaluation
- Risk Treatment
    - Consider mitigation options (Step 5)
- Monitoring and review
- Communication and consultation

[12] FEMA, *Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings,* 2005.

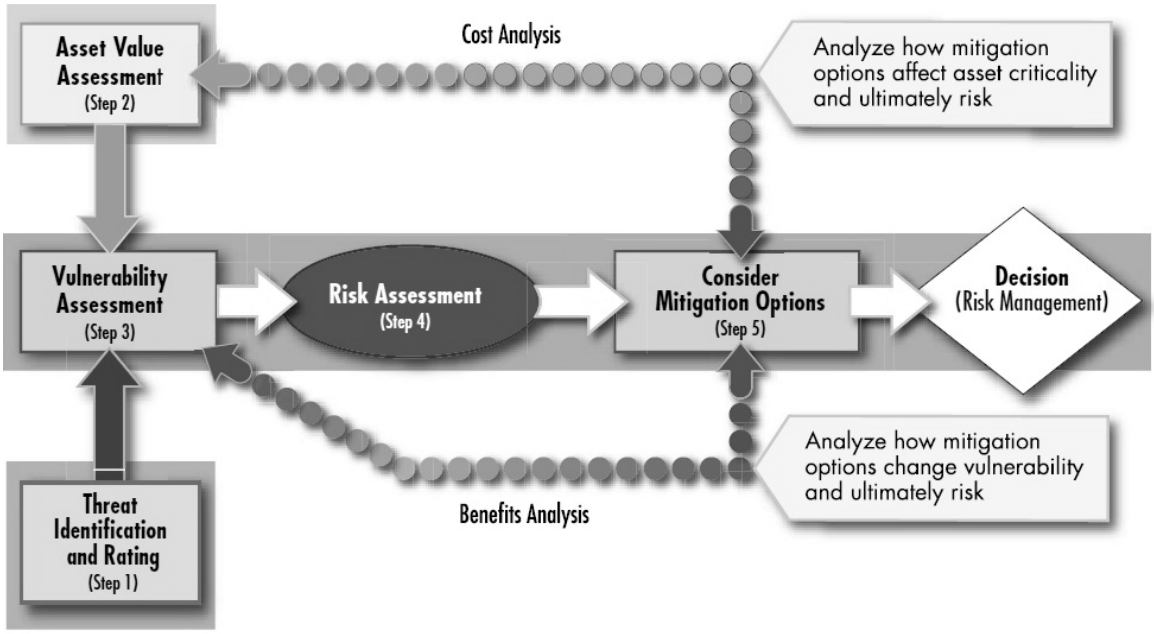

Figure 3: Risk assessment process model[13]

The risk assessment process can help identify the best and most cost-effective terrorism mitigation measures for a building. The model starts with three steps. Step 1 identifies, defines and quantifies the hazard or threat. Step 2 identifies the value of the building's assets that need protection. Step 3 assesses the potential vulnerability of the critical assets of a building. This assessment is also the starting point for determining the possibilities for mitigation measures. Step 4 is the risk assessment itself. In this step, the level of risk is determined for each critical asset for each applicable threat. The combination of the probability of the threat occurring and the possible consequences are considered when looking at mitigation options in Step 5. In this last step, decisions can be made regarding what mitigation options to implement.

Each of the steps consists of multiple tasks that have to be performed. These steps with their tasks lead the researcher through the five steps of doing a risk assessment.

Step 1, threat identification and rating, consists of the following tasks:

1.1 identifying the threats

[13] Ibid, p.iii.

1.2 collecting information

1.3 determining the design basis threat

1.4 determining the threat rating

Step 2, asset value assessment:

2.1 identifying the layers of defense

2.2 identifying the critical assets

2.3 identifying the building core functions and infrastructure

2.4 determining the asset value rating

Step 3, vulnerability assessment:

3.1 organising resources to prepare the assessment

3.2 evaluating the site and building

3.3 preparing a vulnerability portfolio

3.4 determining the vulnerability rating

Step 4, risk assessment:

4.1 preparing the risk assessment matrices

4.2 determining the risk ratings

4.3 prioritising observations in the Building Vulnerability Assessment Checklist

Step 5, consider mitigation options:

5.1 identifying preliminary mitigation options

5.2 reviewing mitigation options

5.3 estimating cost

5.4 reviewing mitigation options, cost, and the layers of defense

The guide discusses what kind of information is needed, how to obtain this information and how to do the calculation of the risk for each selected threat.

For example, within task 1.1 a number of risks are given in a table. These risks can be considered when preparing a risk assessment. For each risk (improvised explosive device, armed attack, chemical agent, biological agent, radiological agent,

cyber-attacks, High-Altitude Electromagnetic Pulse or high power microwave EMP), the application mode, duration, extent of effects and mitigating and exacerbating conditions are described. In task 1.2 the primary threats are selected. This is done using a set of criteria. These criteria can be found in Appendix 1. The criteria are used to rate the different scenarios for the building at hand. For each scenario, the scores on each of the criteria are added, resulting in a total score. An example of the resulting table is given in Appendix 1 as well. These total scores can be used to determine the primary threats. The threat rating mentioned in task 1.4 can then be acquired by using tables (based on scenarios) given in the guide.

Each set of tasks within a step ends with a scenario-based rating that can be acquired from a set of tables. The tables are accompanied by worksheets that can be filled out for the building at hand. The tables for step 2, determining the asset values, and the vulnerability assessment are done in a very similar way to determining the primary threats. A number of criteria are given, describing the relative value of the asset. Next, each criterion is rated for each function of the building combined with each threat. And again, worksheets are offered to help the user fill out the tables for their specific building.

The risk is considered to be the product of asset value, threat rating and vulnerability rating:

Risk = Asset Value * Threat rating * Vulnerability Rating

The risk rating is then determined by a table, in which a distinction is made between low risk, medium risk and high risk, depending on the value of the multiplication.

In task 5.4, a long list of (90) possible mitigation options is given, ordered from less protection / less cost and less effort (for example remove any dense vegetation that may screen covert activity or locate fuel storage tanks at least 100 feet away from all buildings) to greater protection / greater cost and greater effort (for example establish ground floor elevation 4 feet above the ground or use reinforced concrete wall systems in lieu if masonry or curtain walls). The purpose of this list is to provide examples of possible mitigation measures and to give an idea of the relation between protection and cost.

Information needed for the evaluation of effectiveness / efficiency

The team assessing the risk should consist of professionals capable of evaluating different parts of the building. They should together have experience in civil, electrical and mechanical engineering, architecture, site planning and security

engineering. They should also be able to estimate the effect of security and anti-terrorism considerations on a site.

There is no new data needed for doing this analysis. The current situation must be known by the assessment team (state of the building, the way in which it is used, what the effect of certain attacks would be on the building), and then it is just a matter of filling out the worksheets provided by the guide. Judgements have to be made about the applicability of the criteria to the scenarios, building functions, layers of defense, type of infrastructure, etc. The team has to be able to make these categorisations. This means that the main effort should be in composing an expert team. The amount of time and resources necessary for this analysis is quite low compared to, for example, those needed for the RAND analysis (covered later in 3.5).

When the risk assessment is done, decisions can be made about the mitigation options. This decision is made based on a cost-benefit analysis.

The guide stops at choosing the mitigation options. An evaluation of the effectiveness thereafter is not made. There is some kind of feedback loop present in the model, where the costs and benefits of mitigation options are determined, but these are only used to determine what options to choose. When the decision is made what options will be chosen, there is no more feedback as to how effective this choice has been. Of course, the analysis could be done all over again, and then the new analysis can be compared to the old one, to obtain data about the effectiveness of the measures taken.

Advantages / disadvantages

The FEMA Guide is easy to use. It explicitly explains how to do the assessment, and worksheets are provided in which the information can be ordered and values can be assigned to all the risks. These easy-to-work-with worksheets also present the downside of the method – the restricted number of options that can be chosen from limits the specificity of the data obtained. On the one hand this saves time, but on the other hand, this may make choosing an option more difficult, as the building at hand may not exactly fit the category. For example, for the type of site, the choices are: administration / engineering / warehousing / data centre / food service / security / housekeeping or day care. The question then is whether the data you get out of the model is accurate enough. It is unclear how deviations from these standard types should be dealt with. A software application is available that will help you through the whole risk assessment process.

Another disadvantage is that no background information is given in the guide. So it is purely a guide on how to do the assessment. Why certain steps are taken or what their origin is, is not at all explained. Neither are the options from which a choice

had to be made. More background information can be found in another document.[14] This document explains all the different types of buildings, threats, etc. that can be chosen from. However, it still does not refer to any scientific literature about the background of the used methodologies. It does not explain why all the lists that can be chosen from during the assessment are the way they are.

Usefulness for this deliverable

The document indicates that the guide is primarily designed for attacks on buildings, but that it could be adapted for other types of critical infrastructure. It does not, however, indicate how this should be done.

Moreover, the guide is helpful in determining the risk a certain building is in and what can be done to mitigate this risk. It does not really offer any help in determining the effectiveness of surveillance technologies already used. It can, however, help indicate the remaining risk to the building.

§3.4 Center for Disease Control (CDC)

The CDC has developed guidelines for evaluating epidemiologic surveillance systems.[15] Epidemiological surveillance consists of systematic and on-going collection of health data when describing and monitoring a certain health event, followed by analysis and interpretation of this data. This information can then be used to plan, implement and evaluate public health programs. The surveillance data can be used both to determine whether there is a need for a new program or the effectiveness of a program. The updated guidelines address among other things the need for electronic exchange of data, which has become of great importance since the appearance of the original guidelines in 1988. The updated guidelines also have a broader scope. They take into account the stakeholders, integration of the method with other systems, the organisation within which the system operates, etc. Much more context is taken into consideration than in the original version. This makes it even more useful for SURVEILLE, as determining the effectiveness and efficiency of a surveillance technology cannot be done without taking into account the context in which these technologies are used. Changes in this context can now explicitly be incorporated into the reports.

Purpose of the model

[14] FEMA. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. FEMA-426/BIPS-06, edition 2, 2011.
[15] CDC MMWR. *Guidelines for Evaluating Surveillance Systems*, May 1988 & *Updated Guidelines for Evaluating Public Health Surveillance Systems,* July 2001.

"*The purpose of evaluating public health surveillance systems is to ensure that problems of public health importance are being monitored efficiently and effectively."*[16] The goal of the guidelines the CDC gives is to ensure optimal use of public health resources through the development of effective and efficient surveillance systems. The variety in methodology, scope and objectives is stressed, indicating that the strength of the evaluation of surveillance systems depends on the ability to assess these characteristics with respect to the requirements of the system. This means that the evaluation method has to be flexible. The guidelines try to make the evaluation process more explicit and objective.

The evaluation (decision) and treatment part of the risk management model are not described in much detail in the CDC guidelines. The guidelines indicate that the different components are interdependent. This means that the interactions between the components have to be taken into account before recommending changes. The guidelines do not, however, advise or prescribe how to decide between different options, given the evaluation of the surveillance systems. The same holds for the reduction elements. The guidelines do not describe how to increase the effectiveness or efficiency of the evaluated systems.

How does it work?

Like the models described earlier, the CDC guidelines generally follow the risk management cycle. The earlier guidelines do this as follows:

- Establishing the context
    - describe the public health importance of the health event (total number of cases, incidence and prevalence / severity / preventability)
    - describe the system: objectives / health events under surveillance / flow chart
- Risk assessment
    - Risk identification: identification of objectives and components
        - describe the system components: what is the population under surveillance, the time period of data collection, what information is collected, who provides this information, how is the data transferred, how is the information stored, how is the information transferred, who analyses the data, how is the data analysed and how often, how often are reports disseminated and to whom, how are the reports distributed
    - Risk analysis: a quantitative and qualitative analysis of a large number of relevant aspects

[16] CDC MMWR, *Guidelines for Evaluating Surveillance Systems*, May 1988 & *Updated Guidelines for Evaluating Public Health Surveillance Systems,* July 2001, p.3.

- usefulness / simplicity, flexibility, acceptability, sensitivity, predictive value positive, representativeness and timeliness / resources used to operate the system / conclusions and recommendations

In the updated guidelines, some more aspects are added. The asterix (*) indicates the items that are new, compared to the original guidelines.

* Task A. Engage the stakeholders in the evaluation – p.4

Task B. Describe the surveillance system to be evaluated – pp.4–11

1. Describe the public health importance of the health-related event under surveillance –
pp.4-5

   a. Indices of frequency

   b. Indices of severity

   *c. Disparities or inequities associated with the health-related event

   *d. Costs associated with the health-related event

   e. Preventability

   *f. Potential future clinical course in the absence of an intervention

   *g. Public interest

2. Describe the purpose and operation of the surveillance system – pp.5-10

   a. Purpose and objectives of the system

   *b. Planned uses of the data from the system

   c. Health-related event under surveillance, including case definition

   *d. Legal authority for data collection

   *e. The system resides where in organization(s)

   *f. Level of integration with other systems, if appropriate

   g. Flow chart of system

   h. Components of system

1) Population under surveillance

2) Period of time of data collection

3) Data collection

4) Reporting sources of data

5) Data management

6) Data analysis and dissemination

*7) Patient privacy, data confidentiality, and system security

*8) Records management program

3. Describe the resources used to operate the surveillance system – pp.10-11

*a. Funding source(s)

*b. Personnel requirements

*c. Other resources

*Task C. Focus the evaluation design – pp.11-12

*1. Determine the specific purpose of the evaluation

*2. Identify stakeholders who will receive the findings and recommendations of the evaluation

*3. Consider what will be done with the information generated from the evaluation

*4. Specify the questions that will be answered by the evaluation

*5. Determine standards for assessing the performance of the system

Task D. Gather credible evidence regarding the performance of the surveillance system – pp.13-24

1. Indicate the level of usefulness – pp.13-14

2. Describe each system attribute – pp.14-24

a. Simplicity

b. Flexibility

*c. Data quality

d. Acceptability

e. Sensitivity

f. Predictive value positive

g. Representativeness

h. Timeliness

*i. Stability

Task E. Justify and state conclusions, and make recommendations – p.24

*Task F. Ensure use of evaluation findings and share lessons learned – p.25

What information is needed for the evaluation of effectiveness / efficiency?

The guideline does not specifically describe who should do the analysis, but when reading it, a deduction can be made that, similar to the FEMA method, a small team within the organisation with expertise on the method and the organisation should be able to do the analysis. For each of the aspects mentioned above, a number of guiding questions are given that help in analysing the effectiveness and efficiency of each of these aspects.

Advantages / disadvantages

An advantage is that the guidelines are easy to use. The expert team will have no trouble in answering all the guiding questions and getting a comprehensive report about the technology at hand.

A disadvantage is that there are no decision rules provided to decide what technology is more effective and efficient. The team has to decide based on the whole report whether the technology is effective and efficient. Of course, all the guiding questions help to determine to what extent the technology is effective or efficient, but the decision has to be made by the team and may thus be somewhat subjective.

Another disadvantage is that there is no actual comparison made between the alternatives. An extensive description of many aspects of a technique will be described. The goal of this description is to be able to determine the effectiveness and efficiency of this method. The reader has to then compare the reports for the different technologies to make a decision about what technology to choose. The guidelines do not provide a method for doing this.

Usefulness for this deliverable

It is very useful to have an elaborate description of all surveillance technologies in the aspects covered by this method. It allows for a sound comparison to be made between the different possible technologies, which should be the basis for making a

decision. In this sense, the analysis is comparable to that made using the RAND / CONOPS method that will now be described.

§3.5 RAND Corporation

RAND Corporation has developed a methodology for evaluating the operational effectiveness of a specific system – U.S. Air Force remotely piloted aircraft (RPAs).[17]

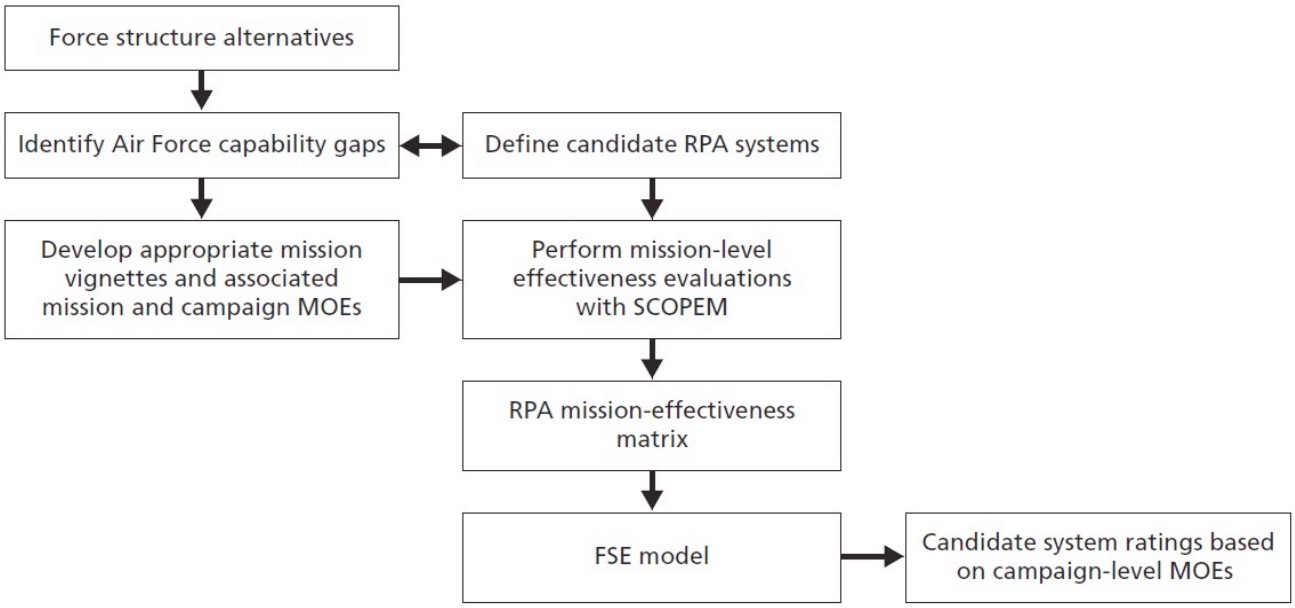

Figure 4. RAND Remotely Piloted Aircraft Evaluation Methodology[17]

This evaluation methodology is specific for the assessment of RPAs so while it does deal with effectiveness (mission and campaign methods of effectiveness, effectiveness evaluations, mission-effectiveness matrix) it does so in a case specific context. The method is nearly fully based on quantification of operational processes. That means that factors like weather conditions, fuel efficiency, fly range and such parameters are quantified and used in computer modelling to estimate just how successful a specific mission for an RPA is. The data-requirements for this evaluation are phenomenal, in the sense that a lot of it is needed but also the level of development of technical models is high. That makes the development of the analysis tool and the analysis itself require a team of scientists to work on this project for a number of years. It is probably costly in development and use.

---

[17] Lingel, S., Menthe, L. Alkire, B., Gibson, J., Grossman, S.A., Guffrey, R.A., Henry, K., Millard, L.D., Mouton, C.A., Nacouzi, G. & Wu, E. *Methodologies for Analyzing Remotely Piloted Aircraft in Future Roles and Missions*. RAND, 2012.

Purpose of the model

The purpose of this model is to demonstrate the work-process for the analysis of the operational effectiveness and cost-effectiveness of unmanned aerial vehicles and other systems that may perform similar tasks. The structured approach forces the analysts to assess the trade-offs between the various candidate systems, missions, technologies and how many missions have to be performed to make the candidate system efficient. As an add-on, the systematic working method helps to identify Air Force capability gaps.

How does it work?

Though the process flow diagram starts (in the left top) with structure alternatives (choices in technology) and the identification of capability gaps, the evaluation of technical systems starts with the development of 'vignettes.' A vignette is a description of the desired delivery of an RPA. Vignettes that are mentioned in the document are: detecting and tracking of a high-value target; suppression of enemy air-defences and destruction of enemy air-defences. Note that a vignette may require more than one technical capability. Long-range flight (as a technical capability) may not be required for high-value target tracking so it is not necessarily part of the vignette. Camera observation, on the other hand, probably is necessary as part of that particular vignette.

The vignette is combined with candidate RPA systems. These candidate systems represent choices of technical systems that could, or might be used for a mission. These choices could include which UAV to use – a Predator, a Wasp or a Raven – and which detectors to install: infra-red cameras or visual spectrum cameras. The selection of technologies and vignettes are combined into a CONOPS description.

A CONOPS description is a standardized reporting structure that is specifically designed for technical systems that require or use masses of data. It is described in IEEE Standard 1362-1998. According to that document a CONOPS should be "a user-oriented document that describes system characteristics of the to-be-delivered system from the user's viewpoint. The CONOPS document is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements (e.g., training, facilities, staffing, and maintenance). It describes the user organization(s), mission(s), and organizational objectives from an integrated systems point of view."[18] The structured reporting makes it easier to compare various candidate systems and forces the analyst to think about technical systems, their application, objectives, complications for organizations etc. The outline of the document is given below.

1. Scope

[18] Thayer RH, Fairly RE & Bjorke P. *IEEE Guide for information technology – System definition – Concept of Operations (ConOps) document*, IEEE Std 1362-1998, 1998.

1.1 Identification

1.2 Document overview

1.3 System overview

2. Referenced documents

3. Current system or situation

3.1 Background, objectives, and scope

3.2 Operational policies and constraints

3.3 Description of the current system or situation

3.4 Modes of operation for the current system or situation

3.5 User classes and other involved personnel

3.6 Support environment

4. Justification for and nature of changes

4.1 Justification of changes

4.2 Description of desired changes

4.3 Priorities among changes

4.4 Changes considered but not included

5. Concepts for the proposed system

5.1 Background, objectives, and scope

5.2 Operational policies and constraints

5.3 Description of the proposed system

5.4 Modes of operation

5.5 User classes and other involved personnel

5.6 Support environment

6. Operational scenarios

7. Summary of impacts

7.1 Operational impacts

7.2 Organizational impacts

7.3 Impacts during development

8. Analysis of the proposed system

8.1 Summary of improvements

8.2 Disadvantages and limitations

8.3 Alternatives and trade-offs considered

9. Notes

The CONOPS descriptions are fed into a quantitative analysis tool called SCOPEM. SCOPEM, in many ways is a marvel of quantitative modelling efforts that is at the heart of this analysis method. Every relevant element in a CONOPS description is modelled with quantified modes. This includes but is not limited to: agent-based modelling of RPAs; weather models; on-board processing capabilities; and the sensitivity of detection. This quantified model estimates the success rate through computer modelling for a mission and thereby its effectiveness. Note that not every mission is a success; factors such as cloud cover and flight altitude can significantly influence the success rate for a mission. From that it follows that the estimate of effectiveness depends on the quality of the (computer) models and the data that is used to model them.

SCOPEM is used to evaluate a number of 'vignette' and technologies combinations, which yields an effectiveness matrix for these combinations. This is represented in the RPA mission-effectiveness matrix.

In the next step of the flow diagram, the FSE model, the SCOPEM model is used to evaluate the effectiveness and efficiency on a campaign level. That is to say, on a level where an expeditionary force or peace-keeping force operates in an area for a number of years. On that level an efficiency estimate is possible where the analysis shows that one vignette-technology combination yields the best use of personnel, energy and operational readiness. The assessment of efficiency is therefore oriented on the maximum yield of a vignette-technology combination with the available resources. The higher the yield, the more efficient the technology is.

What information is needed for the evaluation of effectiveness / efficiency

The information requirement for this method is formidable. Not only does SCOPEM use geographical maps, weather maps, space weather models, cloud models, air-navigation charts and military information, it also requires intricate technical details of the technical systems involved: aeronautical technology, ground stations, communication technology, etc., etc. For the U.S. military, access to technical details of their systems is relatively easy because the systems are built to their

specifications and often developed in their own laboratories. In a commercial vendor-buyer relationship, the sharing of technical details may never be that good. The amount of data and the great variety of technical knowledge to handle that data may only be possible at the state level. It is quite possible that municipalities, individual police forces and crime fighting task forces would never have the manpower to handle such complex technological developments and data requirements.

Advantages / disadvantages

This method has many characteristics of quantitative operations research. That is to say, complex quantitative models model in great detail every part of the vignettes and technologies. Though the quantification of mission success and collecting evidence for further studies often helps analysts to understand their risk system, the level of development as is in this method is probably not required. The staggering data burden and complexity of the model are a disadvantage to the point that it is impossible to use in surveillance for fighting terrorism and serious crime, unless it is an effort supported by significant funds and expertise on a scale only achievable on a national or EU level.

Nonetheless, there are some advantages to the method. Firstly, it demonstrates that a full quantitative analysis is possible; when the surveillance problem is simpler (like monitoring theft) it is a real possibility. Secondly, it follows a structured analysis path that can be used over and over again; this makes the comparison between various technologies easier. In fact, the scheme in figure 2 demonstrates many elements in Roland's value adding circle (§1.5): goals are set, the task is modelled and an evaluation takes place. In that sense, this work supports the Roland cycle. Finally, it makes use of a very sensible tool: CONOPS. CONOPS is a structured way of reporting the intended use of a technology for a specific task; such clarity makes the evaluation for effectiveness (the level of success) and the efficiency (how much work is involved) much easier. The CONOPS report could be a burden for small crime fighting teams but for municipalities it is a suitable tool for clarifying their intentions for surveillance equipment.

Usefulness for this deliverable

This method shows what a fully developed quantitative model for surveillance operations can do. It can predict the performance of technologies in great detail and predict the effectiveness and efficiency of a given technology. However, it was not developed for assessing surveillance technology for surveillance purposes, which limits its usefulness in the present context. Rather, it sets a standard and direction for quantitative technology assessment.

One aspect of particular use in this deliverable is the CONOPS report. It provides assessors with a well-structured report about a technology with clear aims, a description of all relevant aspects and signposts that determine effectiveness and efficiency. The method is tested and tried and described in a clear standard. There are individuals that are experienced in writing such documents so that it is not difficult to learn how to write them.

Another useful aspect is that the entire assessment cycle can be mapped on the Roland cycle (§3.1), which supports the circular value adding cycle for risk. In that sense, this work points to the Roland process model as a useful starting point.

§4 Use of effectiveness and efficiency analysis frameworks in the MerPol Scenario

This section describes the use of effectiveness and efficiency assessment frameworks in a practical application. It would be best if all five methods would be adapted and optimized for use in surveillance technology assessment but that is beyond the scope of this report. Alternatively, an envisaged use is presented that sheds light on the usefulness of the frameworks. Though the method is relatively crude, it provides valuable insight into effectiveness assessment: which elements recur in different frameworks; which framework works better for one technology or another and which is the best overall. These insights are important for the development of an assessment tool in SURVEILLE.

§ 4.1 Testing criteria

The exercise in this report is to assess a number of candidate evaluation frameworks for use in surveillance technology effectiveness (and efficiency). The objective of this exercise is to understand whether the frameworks provide a useful basis for development of an assessment framework for use in SURVEILLE. The following criteria are addressed:

1. Usefulness for the assessment of the effectiveness of surveillance technology;
2. Usefulness for the assessment of the efficiency of surveillance technology;
3. Support for the decision-making process for deployment or selection of surveillance technologies;
4. Efforts required to change the existing framework into a dedicated tool for surveillance technology.

§ 4.2 Testing method

To answer the criteria, an assessment table will be used for each surveillance technology used in the MerPOL scenario. These tables contain the following parts:

1. The technology under consideration, which are selected from the MerPol scenario presented in SURVEILLE deliverable D2.6.
2. What is its purpose in the context of the scenario? In order to determine the effectiveness or the efficiency, the purpose of using the technology in this specific instance has to be known.

3. When the assessment frameworks are applied, how would these frameworks work for this particular technology/framework combination? What would you have to do to perform the assessment and would that be difficult or even possible?

Criterion 4 can only be addressed effectively after all the technologies are treated; this is addressed in §5.

There are 19 technology usage situations discussed in D2.6. They are the following:

1. Visual spectrum dome – zoom, tilt, rotate (public place – used overtly)
2. Visual spectrum dome – zoom, tilt, rotate (public place – used covertly)
3. Covert photography in public places
4. Sound recording bug in target's home
5. Sound recording bug in target's vehicle
6. Sound recording bug on public transport used by target
7. Sound recording bug in police vehicle transporting target following arrest
8. Sound recording bug in target's prison cell
9. Platform micro-helicopter
10. AIS ship location detection and identification
11. Explosives detection near harbour
12. Gas chromatography drugs detector
13. Whole body scanner
14. Luggage screening technology
15. Money laundering technology
16. Networked data analysis
17. Data transfer analysis (name recognition technology?)
18. Location tracking of cellular phones
19. Mobile phone tap

The technologies found in the MerPOL scenario are the following: 1-10, 13, 14, and 16-19. Only technologies 11 (explosives detection near harbour), 12 (gas chromatography gas detector) and 15 (money laundering technology) are not represented in the scenario. Only the technologies from the scenario will be discussed in this paper.

In section §5 below, the specific piece of technology connected to each specific step in the crime investigation, as described by MerPol, will be discussed. The table presents each step of the crime investigation, which piece of technology is used and why, and tests the use of different frameworks to assess the technology. Five frameworks are treated (see §3): the value assessment process, ISO 31,000, FEMA, CDC, and RAND.

§5 Test on the case study of D 2.6 (results)

1. **Information/ Intelligence/ Evidence** Intelligence (low grade) suggests that nominal X is engaged in the large-scale importation of drugs.	**Potential Law Enforcement Activity** Research and analysis, including open source research on X.
Which technology?	Open source research – # 16-17 Data analysis tools
What is the purpose of using this technology?	To find out whether nominal X is related to any other known nominals.
Value analysis process	The value analysis process dictates only a few actions for the technology assessment: set the goal for open source research; describe the resources that are available; analyse the expected results and make a decision (yes/no) to proceed with the open source research. When, after deployment, goals are not achieved or resources are inappropriate, the analysis or decision may be adapted for subsequent uses of open source research.
ISO 31.000	ISO 31.000 demands more details than the value analysis process. A description of the context and risk analysis has to be made before deployment. In this case, the context is that there is a possibility of serious crime. This context partially determines the sense of urgency for the deployment of open source research. Since there is only low-grade intelligence available, a full-fledged risk analysis of the technology is probably disproportionate to the aims. Risk analysis before deployment might be necessary when there are too many cases for the technology to handle. The evaluation of effectiveness and efficiency takes place after the deployment of the technology: was evidence of serious crime found or evidence that there is no crime? How much time/money did it cost to determine this? These lessons learned can be used

	the next time a decision has to be made about this technology; this is the monitoring function in ISO 31.000.
FEMA	The FEMA system is similar to ISO 31.000 except that the risk analysis is primarily coded into point-scoring systems. A structured point-scoring process would be followed where scores are used to classify the threat (seriousness of the crime); the possible losses (to society and/or of assets); vulnerability and risk. The last step (the risk scoring) suggests whether the open source research should be used or whether another technology is more appropriate. Thus, the FEMA model of analysis can be used to choose the appropriate surveillance technology in this step of a crime investigation.
CDC	The CDC method focuses on assessing and comparing surveillance systems beforehand. In this application, the method requires a detailed analysis for the surveillance technology in the given context. A wide range of parameters is required: the risks that may be associated with the crime group currently under evaluation; the precise purpose of the technology; resources; standards for effectiveness and efficiency; direct discussion of the preceding points with all stakeholders. For this step in the crime scenario of MerPol such a detailed analysis is probably disproportional.
RAND / CONOPS	Like the CDC method, this method focuses on assessing effectiveness and efficiency prior to deployment of the surveillance system. However, in this case, a fully quantified model is developed to simulate the physical behaviour of the technology. If it were applied to the selection of open source research the analysis would be oriented towards simulation of physical processes. Since this is primarily an exercise of gathering data, simulation of physical processes is not relevant.

2a. Information/ Intelligence / Evidence	**Potential Law Enforcement Activity**
Intelligence suggests	Commence research and analysis including open

association between nominal X with nominals Y and Z and provides detail of their intention to import controlled drugs.	source research on Y and Z.
Which technology?	Open source research – # 16-17 Data analysis tools
What is the purpose of using this technology?	To determine what information can be found on nominals Y and Z related to their intended import of drugs.
Value assessment process	The same technology is used in 2a as in 1. However, the purpose is somewhat different. This means that the value analysis process has to be adjusted for this step in the scenario. New goals have to be set for the current form of open source research; the available resources have to be described again (these may or may not be the same as in 1); an analysis must be done of the expected results and a decision made (yes/no) regarding proceeding with the open source research. When, after deployment, goals are not achieved or resources are inappropriate, the analysis or decision may be adapted for subsequent uses of open source research. This demonstrates that different goals for open source research can lead to different results related to effectiveness and efficiency.
ISO 31.000	A description of the context and risk analysis has to be made before deployment. The context has now changed somewhat when compared to 1, in the sense that the investigation is now aimed at three persons (nominals X, Y and Z) instead of one (nominal X). More resources may be needed to gain more intelligence on these three nominals. How many people are you willing to investigate to gather the information needed?
FEMA	The structured point-scoring process of FEMA would be followed where scores are used to classify the threat (seriousness of the crime); the possible losses (to society and/or of assets); vulnerability and risk. The last step (the risk scoring) suggests whether the open source research should be used or whether another technology is more appropriate. Thus, the FEMA model of analysis can be used to choose the appropriate surveillance technology in this step of a crime

	investigation
CDC	See 1
RAND / CONOPS	See 1

2b. Information/ Intelligence / Evidence Intelligence suggests association of nominal X with nominals Y and Z, and provides detail of their intention to import controlled drugs.	**Potential Law Enforcement Activity** Development of the intelligence through a covert internet investigation.
Which technology?	Covert internet investigation – # 16-17 Data analysis tools
What is the purpose of using this technology?	To find connections between involved nominals and known suppliers of drugs or weapons.
Value assessment process	First, set the goal for the covert source research: find connections between involved nominals and known suppliers of drugs or weapons. Then describe the resources that are available: time, personnel, etc. Analyse whether the goals can be met within the limits of the resources. After deployment, analyse the success to assess efficiency and effectiveness.
ISO 31.000	The context that sets the urgency is a serious crime investigation in drugs and weapons trafficking where the link to known criminals is investigated. In this phase it is important to establish whether the risk profile of the suspects has changed in respect to earlier findings in the investigation, which justifies this more intrusive surveillance technology. The evaluation of effectiveness and efficiency takes place after the deployment of the technology: was evidence of serious crime found or evidence that there is no crime? This ensures learning for future cases.
FEMA	Part of the analysis that was done in earlier stages of the investigation may have to be repeated. Depending on the outcome from other technologies, the scores may change, thereby changing the level of intrusiveness proportional to using this more intrusive surveillance technology.

CDC	Like the FEMA method, it is important to incorporate changes in the context and/or risks involved for deciding to use another kind of surveillance technology. A wide range of parameters has to be checked to see whether they are still valid: changed risks associated with the crime group; the precise purpose of the covert technology; resources; standards for effectiveness and efficiency; direct discussion of the preceding points with all stakeholders. Historic databases and existing reports following the CDC model as well as CONOPS reports can be used to determine which technologies have been most successful (i.e. effective and efficient) in past investigations, be it local, regional or even (inter)national. These reports can be taken into account when going through the value assessment process and the ISO 31.000 risk management cycle. All models can be taken into account at this stage, assuming that there is the time to do so. Otherwise, analyses that have previously been done for certain scenarios can be compared to the current scenario to make a quicker, but also les comprehensive decision about what kind of technology to use.
RAND / CONOPS	Since covert internet investigations are mainly non-physical, the RAND model is not applicable. The development of a non-physical simulation model is not within the scope of the RAND method.

3. Information/ Intelligence / Evidence Intelligence regarding nominal Z suggests that they are linked to a firearms supplier in another EU member state.	**Potential Law Enforcement Activity** Conduct further and more in-depth research and analysis including open source research on nominal Z.
Which technology?	In-depth research and analysis including open source – # 16-17 Data analysis tools
What is the purpose of using this technology?	Determine whether the link between nominal Z and a firearms supplier can be confirmed.
Value assessment process	See 2a

ISO 31.000	The context is changing a bit in this new development in the scenario, with the suggestion that there is a link with a supplier in another EU member state. This means border crossing activities, and thus possible cooperation with the police in the specific member state and possibly with the states between these two states, in relation to transportation of the goods through them. The effectiveness and efficiency of the technology can be greatly affected, due to time issues, possible communication issues, differences in laws and surveillance technologies deployed, etc.
FEMA	See 2a
CDC	See 2b
RAND / CONOPS	See 1

The following stage in the MerPOL scenario differs from the others in that it is a decision of what kind of surveillance technology to deploy. This consideration comes back a number of times in the scenario. For this purpose, the models we have been discussing thus far can also be used. This table explains how this can be done.

4a. Information/ Intelligence / Evidence Further intelligence suggests the intention of X, Y and Z is to bring a firearm into the country with the future drugs consignment but no further details as yet regarding the date.	**Potential Law Enforcement Activity** Which surveillance technology could be deployed?
Which technology?	All technologies
What is the purpose of using this technology?	Determine what is the best surveillance technology to be used for the current goal.
Value assessment process	Goal and resources have to be very clearly set. This will limit the number of technologies useful for this purpose. Efficiency and effectiveness ratings from past deployments can be used at this stage. If prior information is missing, the assessment may be difficult.

ISO 31.000	Context and risks have to be made very clear. Combined with the results from the value assessment process, a choice can be made for an efficient and effective technology that fits the context, purpose and resources. ISO 31.000 is very useful here since it analyses risks before a choice in methods is made.
FEMA	The structured point-scoring process is followed where scores are used to classify the threat (seriousness of the crime); the possible losses (to society and/or of assets); vulnerability and risk. The last step (the risk scoring) suggests whether open source research should be used or whether another technology is more appropriate. The FEMA method can thus be used when choosing a method of surveillance. However, a list options and associated point scoring is usually prescribed.
CDC	CDC starts by describing the context, which is very important in this instance. A wide range of parameters must be checked to determine their validity in being used to select a surveillance technology. Since this model is specifically designed for the selection of the best method from alternatives, it is very well suited for this particular step of the crime scenario.
RAND / CONOPS	Like the CDC method, the RAND / CONOPS method focuses on assessing effectiveness and efficiency beforehand. However, in this case a fully quantified model is developed to simulate the physical behaviour of the technology. If it were applied to the selection of surveillance technologies, a comparison could be made between the physical processes, for example, CCTV or sound bugs. This would require full modelling for all possible technologies; this is probably beyond the scope of any terrorist or serious crime investigation.

4b. Information/ Intelligence / Evidence	**Potential Law Enforcement Activity**
Further intelligence suggests the intention of X, Y and Z is to bring a firearm into the country with the future drugs	Should the surveillance include the covert use of a public place (overt) CCTV and photography, etc.?

consignment but no further details as yet regarding the date.	
Which technology?	CCTV and photography – # 1-3 CCTV Technology
What is the purpose of using this technology?	Determine whether there is any physical contact between nominals X, Y and Z and other suspicious people.
Value assessment process	The goal for CCTV and photography: determine whether there is any physical contact between nominals X, Y and Z and other suspicious people. The resources available: CCTV, personnel. Note that at this stage, the technology needs to be deployed on-site for surveillance, as opposed to desk research. Analyse whether the goals can be met within the limits of the resources. After deployment, analyse the success to assess efficiency and effectiveness.
ISO 31.000	The context is unchanged from surveillance deployments considered in 4a. The (risk) analysis is for the justification of the use of CCTV and photography. The effectiveness and efficiency of the equipment can be evaluated following the surveillance: was there physical contact between suspects? At what time is the shipment? Was the operation expensive? The relatively simple choice between two similar technologies probably does not require a full risk analysis.
FEMA	By this time, the point system of the FEMA method would have been updated from prior stages in this crime investigation. The analysis that follows should suggest (or allow) the use of CCTV and photography. It is possible, however, that a system based on points does not distinguish well between technologies that are similar. In addition, the FEMA method would also suggest alternative surveillance technologies.
CDC	See 2b. When the context or purpose of the investigation changes, these changes need to be incorporated in the CDC reports for future reference. The context description ought to be relatively well done in this phase of the investigation but it would be hard to distinguish between technologies that are relatively similar in nature.

RAND / CONOPS	Since this is the first use of evidence in a physical environment the RAND model becomes relevant. However, the requirements are demanding: construct a physical model for optimal deployment of CCTV or photography; detect obstacles; incorporate technical failure, quality of the recordings and degeneration by post-processing. This model could make very precise calculations on which of the two similar technologies performs best; it could even disclose the effectiveness and possibilities of failure in absolute terms.

4c. Information/ Intelligence / Evidence Further intelligence suggests the intention of X, Y and Z is to bring a firearm into the country with the future drugs consignment but no further details as yet regarding the date.	**Potential Law Enforcement Activity** Should law enforcement commence financial background enquiries and development of financial profiles on all nominals?
Which technology?	Financial background enquiries and financial profiles – # 16-17 Data analysis tools
What is the purpose of using this technology?	Determine whether there are any suspicious financial transactions made by nominals.
Value assessment process	See 2a
ISO 31.000	See 2a
FEMA	See 2a
CDC	See 2b
RAND / CONOPS	See 1

6a. Information/ Intelligence / Evidence Surveillance identifies a male believed to be a foreign national who is	**Potential Law Enforcement Activity** Should law enforcement intensify observations / surveillance on the home address of Z to identify the foreign national?

regularly visiting the home address of Z and appears to be staying over night. It is suspected that this may be the firearms supplier.	
Which technology?	# 1-3 CCTV Technology
What is the purpose of using this technology?	Determine identity of the male visiting the home address and determine whether he has anything to do with the intended purchase of drugs or a firearm.
Value assessment process	The goal for CCTV and photography: determine the identity and reasons for the visiting male and determine whether he has anything to do with the intended purchase of drugs or a firearm. The resources available: CCTV, personnel. Note that at this stage, the technology needs to be deployed on-site for surveillance, as opposed to desk research. Analyse whether the goals can be met within the limits of the resources. After deployment, analyse the success to assess efficiency and effectiveness.
ISO 31.000	The context is changed somewhat from previous surveillance deployments in this case. Now there is a new suspect and intensifying the observations / surveillance may create a better image of the events at the target's home address.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

6b. Information/ Intelligence / Evidence	**Potential Law Enforcement Activity**
Surveillance identifies a male believed to be a foreign national who is regularly visiting the home address of Z and appears to be staying over night. It is suspected that	Should law enforcement consider deployment of covert CCTV and maintain general surveillance?

this may be firearms supplier.	
Which technology?	# 1-3 CCTV Technology
What is the purpose of using this technology?	Determine whether there are any other suspicious activities at target's home address besides those concerning the foreign national.
Value assessment process	The goal for CCTV and photography: determine whether there are any other suspicious activities at target's home address besides those concerning the foreign national. The resources available: CCTV, personnel. More resources may be necessary than for the surveillance described in 6a, as it is unclear what they are looking for; it is a more general search for intelligence. It is difficult to determine the effectiveness and efficiency when describing a goal in this manner. As it is unclear what they are looking for, it is difficult to determine whether the surveillance has been successful.
ISO 31.000	The context has not changed from 6a. The scope, however, has broadened from being interested in one individual to a more general search for suspicious activities. At this point, the risk of disclosure enters the risk analysis as a concern.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

7. Information/ Intelligence / Evidence	**Potential Law Enforcement Activity**
The home address for Z is in a rural location making general surveillance by a team and the deployment of covert CCTV extremely difficult.	Consider covert use of drone and / or other air surveillance in order to maintain observations.
Which technology?	Drone and / or other air surveillance – # 9 Platform micro helicopter

What is the purpose of using this technology?	The goal of air surveillance is the same as the goal was for CCTV.
Value assessment process	The goal for using a drone or other air surveillance is the same as it was for using covert CCTV, but the CCTV turned out not to be effective, due to the rural location of target's home. The resources required for use of the drone, however, are very different. This means that a new analysis of the effectiveness and efficiency is necessary.
ISO 31.000	The context is unchanged from earlier surveillance deployments in this case. The (risk) analysis for the justification of the use of a drone may give different results. Again, probabilities of failure of the operation also come in to play here.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

8a. Information/ Intelligence / Evidence Further intelligence is received that the drugs / firearm importation is imminent but there are no further details as to the route to be taken. The source is not likely to be able to assist any further.	**Potential Law Enforcement Activity** Consider use of covert listening device at home address and / or vehicle of Z.
Which technology?	Covert listening device at home address and or vehicle of Z – #4-5 Sound recording bug in target's home address / vehicle
What is the purpose of using this technology?	Determine the route that will be used to transport the drugs / firearm.
Value assessment process	The goal for using a sound recording bug: to listen to the conversations at the home address and in the car of Z, in order to determine the intended route for importing the drugs and / or firearm into the country.

	As with most of the other technologies, the effectiveness and efficiency can only be determined afterwards. Has the use of this technology led to the desired information needed for the case?
ISO 31.000	In this case a risk analysis is important, as physical access has to be gained to both the home and the vehicle of nominal Z to install the sound bugs. Is this risk justifiable, or should other technologies be preferred?
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

8b. Information/ Intelligence / Evidence Further intelligence is received that the drugs / firearm importation is imminent but there are no further details as to the route to be taken. The source is not likely to be able to assist any further.	**Potential Law Enforcement Activity** Should law enforcement start to consider interception of communications?
Which technology?	Interception of communications – # 18-19 Location tracking of cellular phones / mobile phone tap
What is the purpose of using this technology?	To determine the intended route for the importation of the drugs and / or firearm.
Value assessment process	The goal is the same, but there is now more time pressure, as it seems that the importation is going to happen at any moment. This makes it more important to listen in on all conversations by nominal Z and his contacts. Not only in his home and car, but also at other locations, when he is using his cell phone.
ISO 31.000	The context changes somewhat, in the sense that the scope is broadening. The increased time pressure indicates that at this moment, all communications could contain important information about the

	imminent import. Moreover, a risk analysis may be interesting, as it is unclear whether nominal Z uses only one cell phone.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

9. Information / Intelligence / Evidence Through surveillance it has been ascertained that whilst travelling with the visiting foreign national, nominal Z quite often uses public transport.	**Potential Law Enforcement Activity** Consider use of covert listening device on public transport.
Which technology?	Covert listening device – #6 Sound recording bug on public transport used by target
What is the purpose of using this technology?	To determine what nominal Z and visiting foreign national are talking about, and to determine whether they are in contact with others.
Value assessment process	The goal of using a covert listening device on a bus is to determine whether the individuals under investigation are associating and if so, what they are talking about. The resources include not only surveillance equipment and personnel to operate it, but also the cooperation of the transportation company and possibly some more external partners. Analyse whether the goals can be met within the limits of the resources. After deployment, analyse the success to assess efficiency and effectiveness. In this case, the environment for the listening device might not be optimal: there is a lot of background noise and the recording device(s) has (have) to be on the right bus. Prior experience will be useful in the assessment of efficiency and effectiveness.
ISO 31.000	In this particular application, a risk analysis may be useful because the environment is not supportive for the use of sound recording devices; buses are noisy, there are many buses and the individuals might be in the wrong place on the bus. Therefore, in addition to the steps taken before in this crime investigation, a mild form of risk analysis is justified.
FEMA	Using the FEMA model would be possible at both early and later stages in the decision-making. A team of experts is needed, but a small amount of data is necessary to decide whether this technology would be usable for this purpose. See 4b.

CDC	See 2b. As with the FEMA method, the context in which the technology is operating should be understood before judging the effectiveness / efficiency.
RAND / CONOPS	Using the RAND model and making a CONOPS for the sound recording bug on public transport would require a large amount of data. The sound bug itself could be analysed without much difficulty, but the context in which it is used has to be taken into account, as this has tremendous effect on both the effectiveness and efficiency of the technology. This could be done in advance, but not at the moment the decision is made whether or not to use this technology. In the CONOPS all possible uses of a technology have to be added, to make sure that any situation at hand can be found in the CONOPS. See 4b.

14a. Information/ Intelligence / Evidence Z and the unidentified foreign national begin to frequently use air travel on the lead-up to the intended date of the importation.	**Potential Law Enforcement Activity** Should law enforcement make targeted use of body scanners at airports against nominal Z and the foreign national?
Which technology?	# 13 Whole body scanner
What is the purpose of using this technology?	Determine whether nominal Z and the foreign national have anything on their body that could also be used in the import of the drugs and or firearm.
Value assessment process	The goal of the whole body scanner: to determine if nominal Z and the foreign national actually have something on their body during these flights that they may want to use when importing the drugs and or firearm. If they just flying abroad to meet with the people with whom they are planning this import, the technology may not give the police any useful information. On the other hand, the resources needed to gather this information may be so low that it is worth looking into, even when the chances of finding something are slim to none.

ISO 31.000	A consideration here could be whether the police would want to have access to the data from the body scanner. On the other hand, there is an intrusion of the privacy of the nominal and the foreign national. Moreover, when the police have to be physically present at the body scanner (depending on whether images are allowed to be stored by the airport), there may be a chance of being noticed by the nominal or foreign national.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

14b. Information/ Intelligence / Evidence Z and the unidentified foreign national begin to frequently use air travel on the lead-up to the intended date of the importation.	**Potential Law Enforcement Activity** Should law enforcement make targeted use of x-ray / scanning machines against any luggage belonging to nominal Z and the foreign national?
Which technology?	# 14 Luggage screening technology
What is the purpose of using this technology?	Determine whether nominal Z and the foreign national have any objects in their luggage that could give more information about the intended import.
Value assessment process	Like in 14a, this seems to be only a question of resources. There is a possibility that this surveillance technology may give valuable information. So when necessary resources are low to obtain this information, the technology can be used to determine if the subjects are carrying anything of importance with them.
ISO 31.000	See 14a
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

15. Information/ Intelligence / Evidence Intelligence suggests that the intended method of importation for the drugs and guns is via sea.	**Potential Law Enforcement Activity** Should law enforcement make targeted and proactive use of ship tracking equipment and harbour scanning devices?
Which technology?	# 10 AIS ship location detection and identification
What is the purpose of using this technology?	Determine which ship is carrying the drugs and / or firearm.
Value assessment process	The goal is to determine which ships might likely be carrying the drugs and or firearm (based on earlier intelligence and information) and after this has been determined, to follow the movement of this ship. Resources are low for the second part, but determining what ship the goods are on may be more difficult. This has to be determined based on earlier information concerning the intended route, country of origin, etc.
ISO 31.000	The risk of this technology is most likely low, as the ships will not be aware of being followed by this tracking system.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

16. Information/ Intelligence / Evidence Arrest	**Potential Law Enforcement Activity** Should law enforcement consider the use of listening devices in cells / police transport?
Which technology?	# 7-8 Sound recording bug in police vehicle transporting target following arrest / in target's prison cell
What is the purpose of using this technology?	Determine all people that have been involved in the import of the drugs and / or firearm and how the whole process has been arranged. To learn for future

	instances.
Value assessment process	The goal of using this technology is to determine whether the suspects talk about anything that may help the police in this case. Personnel are needed to listen to all conversations in the cell and police transport.
ISO 31.000	The context has changed.
FEMA	See 4b
CDC	See 2b
RAND / CONOPS	See 4b

§6 Discussion

§ 6.1 The MerPol Scenario

The MerPol crime investigation scenario has been very helpful in comparing different frameworks for assessing effectiveness and efficiency and how the frameworks could work in practice. Not only does the scenario clearly state objectives, which is necessary for any efficiency and effectiveness assessment; it also demonstrates that a number of technologies are used in various stages of the investigation (e.g. photography, CCTV and sound recording) and that sometimes more exotic equipment is called for. In addition to demonstrating how the assessment frameworks can be used, the scenario reveals where their strengths and weaknesses lie.

Roland's value assessment process provides a fairly straightforward analysis framework that can be employed at any step of the crime investigation scenario. It is strongly tied to independent decisions and considerations in the scenario and provides a framework for making these decisions. Thus, this process is used over and over again. However, each decision invokes its use anew and each time, prior knowledge must be sought for that particular problem. For a useful effectiveness and efficiency assessment, prior knowledge would have to be stored for later use which means that a large number of different decision processes would have to be categorized and stored. This method is, to some extent, comparable to the normal practice in crime investigations where surveillance operations have to be justified for every operation. For that reason, it would be useful to consider using this system in SURVEILLE.

ISO 31.000 is more complex and more adaptive than the value assessment process. It requires an initial risk assessment before decisions are made. That is to say, at the start of the investigation some energy will be spent on the construction of a crime risk profile in a particular context. As the investigation progresses the risk model will need to be adapted, updated and sometimes rigorously tested before a decision. This working process enables more diverse decisions than the value assessment process. When the ISO framework is used, the efficiency and effectiveness assessment is strongly coupled to the case (and can be compared with other cases). Where the value assessment process is useful in decision-making and efficiency discussions about a specific technology to answer as specific crime investigation question, the ISO method also allows for selecting the better technology from a spectrum of technologies, and more clearly incorporates chances of failure of an operation. That is to say, efficiency and effectiveness assessments may be made based on crime cases rather than individual decisions. The risk management cycle is rarely part of crime or terrorist investigations but it could improve the normal operation in a crime investigation. In SURVEILLE such analysis strategies could pave the way for future investigations.

The FEMA method is a semi-quantitative method based on ISO 31.000 but with several parameters being fixed as numbers. In that sense, it is not very different from the assessment method described in D2.6 of the SURVEILLE project. An advantage over the ISO method is that once the initial risk analysis (or point-setting) is performed, while the numbers may change during the crime investigation, the framework remains the same, and repetitive decisions do not require additional analysis. This makes FEMA easier to use than ISO. It is, however, less versatile as, only technologies, risks, costs or other factors that have been quantified can be used, and adding new parameters may be difficult. With this method, a number of similar cases may be grouped together for the analysis of efficiency and effectiveness. Lessons learned may also be used to adapt point values in the assessment method. Prior to any analysis, the point system has to be developed per (type of) crime investigation case. That may require a considerable research effort that would take place outside the normal crime investigation process. Note the point-scoring system used in deliverable D2.6 of the SURVEILLE project.

The CDC method is focused on assessing technology before deployment. Also, it is strong in determining which of a number of technologies would be best in a given context. Such an assessment could be useful in crime investigations but the assessment would require a significant research effort in a crime investigation case. That makes it unlikely to be used as it is, but selected technologies could be assessed on a national or international scale. This effort could be worthwhile in the SURVEILLE project. Note that the method is purely qualitative. The lack of quantitative information makes the predictions for efficiency and effectiveness rather broad.

The RAND method is the most complete assessment tool from the five that were assessed. It is a fully quantified model that incorporates all physical aspects for the use of a technology. It includes a quantified description of the operation environment, weather conditions, human performance, technical capabilities and more. For each type of technology a fully quantified model would have to be designed: for sound recording, phone tapping, CCTV, radar. The investment costs would be formidable but once a model exists that is coded in a computer program it would be relatively easy for a police force to use the program. Such a program would yield detailed insight into the success rate of a piece of technology and could be used to optimize surveillance strategies within a given space. Also, the predictions would be accurate and precise. However, the development of a fully quantified model is beyond the scope of the SURVEILLE project and will therefore not be considered in this report.

Our analysis of these different models indicates that the complexity of the assessment framework increases. The more complex a model, the more time and effort is required to prepare the assessment method for use, the more money it will cost to develop the assessment method for application in surveillance, but also, the more accurate or trustworthy the outcome will be. Note that effectiveness

assessments in Roland, ISO and FEMA are primarily based on prior knowledge and experience of surveillance technologies, and that CDC and RAND are designed for the prediction of efficiency and effectiveness.

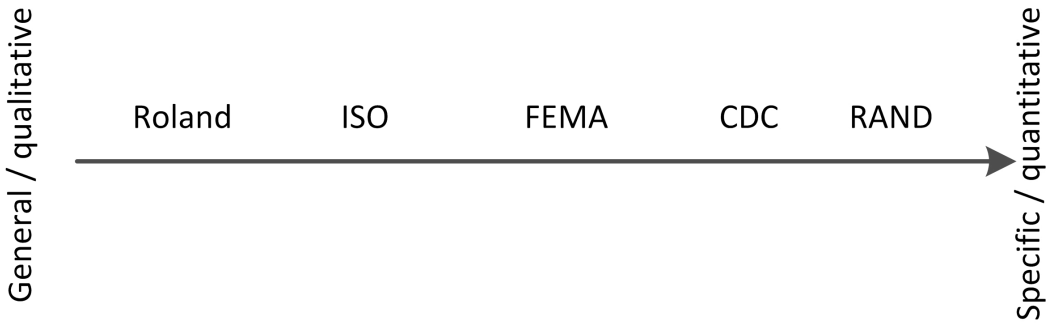

Figure 5. Complexity of the 5 models discussed in this deliverable

§ 6.2 Testing criteria

The review of the MerPol scenario provides insight into whether the candidate evaluation frameworks meet the testing criteria provided in §4. The criteria are treated below in numerical order.

1. Usefulness for the assessment of the effectiveness of surveillance technology

All five methods can be useful for the assessment of effectiveness; that is to say, all methods fulfil criterion 1. This should not be surprising since this assessment was one of the criteria to consider them in the first place. The RAND method is by far the most capable of assessing effectiveness; it can do so accurately and precisely. Roland and ISO depend heavily on prior knowledge of effectiveness; once such prior knowledge is available, estimates of effectiveness may be quite accurate. The FEMA method depends on prior knowledge but it is coded in a semi-quantitative point-scoring method. That makes it easier for use in the assessment of effectiveness but also makes it coarse in its estimates. The CDC method is also relatively coarse in its predictions but it does not depend on prior knowledge as much as Roland, ISO or FEMA.

2. Usefulness for the assessment of the efficiency of surveillance technology

For an assessment of efficiency, effectiveness is a prerequisite. If a technology is not effective in any way, any effort spent is inefficient. If a technology is fully effective, the cheaper option is more efficient. If the effectiveness is 50%, efficiency becomes a difficult concept. The latter is the case for the CDC method. Since it is based on relatively coarse, mostly non-quantitative information, the estimate for effectiveness is coarse, which makes the assessment of efficiency unclear (but not impossible). The RAND method is, once again, the best predictor for efficiency; it is built into the QRA model. And similar to effectiveness, the Roland and ISO methods, the correctness of the assessment depends on the quality of prior knowledge. The FEMA method provides an extra tool that makes efficiency assessment easier: it is particularly well suited to make choices between different sets of technology, thereby rendering it easier to choose the cheapest one. In conclusion, all methods can be used to evaluate efficiency but RAND is the most precise and CDC is the most imprecise, whereas the other three methods depend on prior knowledge for successful application.

3. Support for the decision-making process for deployment of surveillance technologies or selection of surveillance technologies

This is where large differences appear between the methods. Roland's value analysis process is directly applicable for crime investigations in its current form; it fits the MerPol scenario directly and can be used over and over again. The ISO method is an extension to that system, with a risk analysis being carried out and updated during the investigation. This requires some extra work for the investigators but provides guidance for future steps of the investigation. When risk profiles change it would be easier to see which more intrusive surveillance tools would be justified. In this sense, it is also fairly easy for investigation teams to use this system for the decision-making process. The FEMA framework does almost the same thing but some precision is lost in favour of a generic decision-making framework that can be used over and over again for investigations of a certain type, while keeping room to manoeuvre for individual investigation teams. The FEMA method, however, requires prior research to build the framework, which, typically, takes place outside the investigation team. The CDC method yields documents that can be used for guidance in operational crime investigations. It provides considerations and estimates but does not necessarily fit the context of a given investigation. Such an assessment is useful for setting standards or harmonizing work processes but would probably not support decision making by crime researchers. Law and policymakers, however, would benefit for such documents for their decision making. The RAND method, if fully implemented, could support local decision making AND national harmonisation; however, the staggering cost could be a problem even on a national level.

4. Efforts required to change the existing framework into a dedicated tool for surveillance technology

All of the frameworks that were described have to be adapted for use as tools for surveillance technology assessment. The effort this would take is more or less comparable to the complexity of the model. So the value analysis process is the easiest to adapt and the RAND model the most difficult. In fact, justification procedures for the use of surveillance equipment in many European jurisdictions already follow such a process. It is fair to conclude here that the RAND model is not a viable method for the SURVEILLE project. Development of fully quantified models takes years and several millions euros. The FEMA method, based on semi-quantitative point scoring is already under development in the SURVEILLE project (deliverable D2.6). This path requires in-depth analysis for the rationale of point scoring but that is possible in the SURVEILLE project. The CDC method would require a considerable effort since an extensive report would have to be constructed for each technology (or maybe a smaller selection). The method is also well suited for the SURVEILLE project for decision making on a high abstract level but it would be difficult to cover a large number of technologies. Both the value analysis process and the ISO process yield methods that could be transformed into useful tools for practitioners; arguably, parts of them are already used today. However, the SURVEILLE project focuses on decision support while balancing human rights, ethical considerations and usability of surveillance technologies. Therefore these frameworks will not be pursued in the SURVEILLE project.

§7 Conclusion

§ 7.1 Summary of conclusions

This report focuses on a systematic approach for the appraisal of effectiveness and efficiency of surveillance technologies. Three main conclusions follow from this report:

- There are no clear definitions for the effectiveness and efficiency of surveillance technology, therefore they were developed for use in SURVEILLE;
- Though there are no clear frameworks for effectiveness and efficiency assessment, at least five model frameworks from other domains provide templates for the development of such frameworks;
- The framework described by FEMA provides a framework that is best suited for further development in the SURVEILLE project.

§ 7.2 Definitions for effectiveness and efficiency

It was found that literature does not provide clear definitions of effectiveness and efficiency for surveillance technologies. Definitions for use in the SURVEILLE report were developed, they are:

Effective surveillance technology has the technical capacity to deliver the intended security goals, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome.

Efficient surveillance technology delivers the intended security goals with low use of resources in terms of cost, time and/or physical and mental efforts.

§ 7.3 Analysis frameworks

Five analysis frameworks were analysed in this report: the value assessment process by Roland, ISO 31.000, FEMA, CDC and RAND. Though these frameworks are from domains other than that of surveillance technology, they show that analysis frameworks for efficiency and effectiveness range from relatively straightforward qualitative frameworks to very complicated quantitative frameworks. It is important to select the right complexity level for use in the SURVELLANCE project. Note that none of the frameworks are directly applicable to surveillance technology

assessment. The method that is selected has to be transformed for surveillance technology assessment.

§ 7.4 Framework for SURVEILLE

The analysis in this report shows that the semi-quantitative crime risk scoring method of the FEMA method is best suited for further development in the SURVEILLE project. With this framework, effectiveness/efficiency research findings can easily be retained in the scoring system, the framework is relatively easily interpreted and the framework is flexible enough for discussion when a point-scoring exercise is performed.

This finding is supported by the findings in SURVEILLE deliverable D2.6 where a point-scoring system is used to replace a simple 'trade-off' between human rights and technology usability The FEMA report provides additional insight into the further development of that assessment instrument.

Further research in work package 3 of SURVEILLE will focus on the development of a point scoring method of which the FEMA framework is an example and the decision matrix in D2.6 is the template.

Appendix 1: FEMA

Criteria							
Scenario	Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building
9-10	Readily available	Basic knowledge/open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	> 5,000	Within 1,000-foot radius
6-8	Easy to produce	Bachelor's degree or technical school/ open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	1,001-5,000	Within 1-mile radius
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence publish/well-known	Controlled access, protected entry	251-1,000	Within 2-mile radius
1-2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Within 10-mile radius

Figure 6. Criteria to determine the primary threats[19]

[19] FEMA, *Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings,* 2005, p.1-21.

Scenario	Criteria: Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building	Score
Improvised Explosive Device (Bomb)								
1-lb. Mail Bomb	9	9	3	8	3	10	1	43
5-lb. Pipe Bomb	9	9	3	8	3	10	2	44
50-lb. Satchel Bomb/Suicide Bomber	8	8	6	8	3	10	3	46
500-lb. Car Bomb	6	8	7	8	3	10	3	45
5,000-lb. Truck Bomb	4	8	5	8	3	10	3	41
20,000-lb. Truck Bomb	2	6	1	8	3	10	3	33
Natural Gas	2	8	1	8	3	10	5	37
Bomb/Aircraft/Ship								
Small Aircraft	9	6	3	8	3	10	3	42
Medium Aircraft	5	4	7	8	3	10	3	40
Large Aircraft	2	3	7	8	3	10	3	36
Ship	0	0	0	8	3	10	3	24
Chemical Agent								
Choking: Chlorine	5	7	2	8	3	10	2	37
Choking: Phosgene	3	10	2	8	3	10	1	37
Blood: Hydrogen Cyanide	3	8	2	8	3	10	1	35
Blister: Lewisite	3	6	2	8	3	10	1	33
Nerve: Sarin	3	4	6	8	3	10	4	38

Scenario		Criteria: Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building	Score
Biological Agent									
Bacteria	Anthrax	4	5	9	8	3	10	2	41
	Plague	4	5	3	8	3	10	2	35
	Tularemia	4	5	2	8	3	10	2	34
Viruses	Hemorrehagic Fevers	4	5	2	8	3	10	2	34
	Smallpox	2	5	2	8	3	10	2	32
Toxins	Botulinum	5	5	5	8	3	10	2	38
	Ricin	8	8	9	8	3	10	2	48
Radiological Agent									
"Dirty Bomb"		5	7	1	8	3	10	5	39
Spent Fuel Storage		2	6	1	8	3	10	1	31
Nuclear Plant		1	6	1	8	3	10	1	30
Armed Attack									
RPG/LAW/Mortar		4	5	2	8	3	10	2	34
Ballistic		10	10	5	8	3	10	2	48
Cyber Attack									
Worm		9	10	5	8	3	10	1	46
Virus		9	10	5	8	3	10	1	46
Denial of Service		9	7	5	8	3	10	1	43

Figure 7. Example of rating, using the criteria to determine the primary threats[20]

Appendix 2: MerPOL scenario (replicated from D2.6)

SURVEILLE Project - Scenario by MerPOL

For Use By SURVEILLE Partners In Consideration Of Types Of Technology, Efficient And Effective Deployment & The Associated Legal & Ethical Issues.

[20] Ibid, pp.1-22 – 1-23

Information / Intelligence/ Evidence		Potential Law Enforcement Activity
Intelligence (low grade) suggests that nominal X is engaged in the large scale importation of drugs		**Decide** – Commence research and analysis including open source research on X? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not?
Intelligence suggests association between nominal X with nominals Y and Z and provides detail of their intention to import controlled drugs.		**Decide** – Commence research and analysis including open source research on Y and Z? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not? **Decide** - Consider development of the intelligence through a covert internet investigation? **Consideration** – Does this additional action by Law Enforcement require authorisation(*) or not?
Intelligence regarding nominal Z suggests that they are linked to a firearms supplier in another EU member state		**Decide** - Conduct further and more in-depth research and analysis including open source research on nominal Z? **Consideration** – Does this action by Law Enforcement require authorisation(*) or not? **Decide** - Commence liaison with other EU member state regarding potential firearms supplier? **Consideration** – Is an ILOR required as yet, is this a formal request for intelligence / evidence at this stage, is law enforcement action sought by other member state at this stage?

		Decide – Should law enforcement 'Friend Request' nominals on open source to develop intelligence relating to X, Y, Z and unknown foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Further intelligence suggests the intention of X, Y and Z is to bring a firearm into the country with the future drugs consignment but no further details as yet regarding date.		**Decide** – Should law enforcement place X, Y and Z under physical observation by Surveillance Team? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should the surveillance include the covert use of use of public place (overt) CCTV and photography etc.? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** – Should law enforcement commence financial background enquiries and development of financial profiles on all nominals?
		Consideration - Does this additional action by Law Enforcement require authorisation(*) or not?
For approximately 3 months there is no development in the intelligence or information being received, nor any		**Decide** - Should the law enforcement operation continue?

intelligence or evidence being obtained from the surveillance operation		**Consideration** - An issue for consideration by the Authorising Officer and investigation team regarding the proportionality, justification and necessity of maintaining covert surveillance.
Surveillance identifies a male believed to be a foreign national who is regularly visiting the home address of Z and appears to be staying overnight. It is suspected that this may be the firearms supplier.		**Decide** - Should law enforcement intensify observations / surveillance on the home address of Z to identify the foreign national? **Consideration** - What surveillance technology could be deployed?
		Consideration - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should law enforcement consider deployment of covert CCTV and to maintain general surveillance? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide** - Should enquiries be progressed / escalated with other EU member state to request specific intelligence and any relevant evidence on the as yet unidentified foreign national? **Consideration** – Is an ILOR required at this stage?
The home address for Z is in a rural location making general surveillance by a team and the deployment of covert CCTV extremely difficult.		**Decide** - Should law enforcement require surveillance to be maintained? **Consideration** - What surveillance technology could be deployed? **Decide** – Consider covert use of drone and / or other air surveillance in order to maintain observations.

		Consideration – Does this additional action by law enforcement require authorisation (*) or not?
Further intelligence is received that the drugs / firearm importation is imminent but there are no further details as to the route to be taken. The source is not likely to be able to assist any further.		**Decide -** Consider use of covert listening device at home address and / or vehicle of Z? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
		Decide - Should law enforcement start to consider interception of communications? **Consideration** - What surveillance technology could be deployed? **Consideration** – If progressed, on which nominals in this scenario? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Through surveillance it has been ascertained that whilst travelling with the visiting foreign national that nominal Z quite often uses public transport?		Is this action by nominal Z and the unknown foreign national deliberate, in order to maintain anti-surveillance activity? **Decide -** Consider use of covert listening device on public transport? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Open source research suggests a link between nominal Z and a crime group engaged in gun crime including armed		**Decide** – does this intelligence justify more intrusive surveillance?

robbery and a gang dispute involving previous shootings.		**Decide -** Should there be research conducted on the intended recipients of the gun? **Decide -** Does this intelligence create a credible threat to life? **Decide -** When should law enforcement move into taking overt enforcement action? **Consideration** - Does any additional action by Law Enforcement require authorisation(*) or not?
Intelligence determines the planned route for importation and an expected date.		**Decide -** Consider liaison with relevant member states regarding surveillance / possible enforcement activity? **Consideration** - Is an ILOR now required requesting specific activity by foreign law enforcement, deployment of investigating officers from another member state and / or introduction of evidence from one country into another's Courts? **Consideration** - Should there be surveillance by law enforcement in another member state? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not?
Intelligence suggests that members of the crime group that are to take ownership of the gun are intending to shoot a named person.		**Decide -** Is there now a credible threat to life situation? **Decide –** Should law enforcement now consider: - Formal warning to intended victim? - Formal warning to possible offenders? - Use of surveillance technology in dealing with this aspect of the operation?

		Consideration - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not?
The intelligence now in possession of law enforcement provides detail of: • The importation of a consignment of drugs and a firearm. • The known route of the importation. • The date of the importation. • The intended recipients of the gun and their intentions.		**Decide –** - Should law enforcement take action at the border / port when the consignment and gun are leaving the originating country? - Should law enforcement take action at the border / port on entering intended country? - Should law enforcement allow the consignment to progress to exchange between couriers and ultimate recipient of drugs / guns / both? **Risks:** - Will the intelligence and surveillance operation allow for certainty as to when the drugs / gun are present? - Will early action lead to no result - Will delayed action result in the gun / drugs being missed? - Is there a risk of losing control of the nominals involved and thereby the gun and drugs? - Will action by law enforcement at any stage compromise intelligence sources? - What impact will the decision to take action / not take action have on the threat to life situation?

Z and the unidentified foreign national to frequently use air travel on the lead up to the intended date of the import.		**Decide -** Should law enforcement make targeted use of body scanners at airports against nominal Z and the foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not? **Decide -** Should law enforcement make targeted use of x-ray / scanning machines against any luggage belonging to nominal Z and the foreign national? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Intelligence suggests that the intended method of importation for the drugs and guns via sea		**Decide -** Should law enforcement make targeted and proactive use of ship tracking equipment and harbour scanning devices? **Consideration** - Does this additional action by Law Enforcement require authorisation(*) or not?
Arrests		**Decide –** Should law enforcement consider the use of listening devices in cells / police transport? **Consideration** - What surveillance technology could be deployed? **Consideration** - Does any additional action by law enforcement abroad require authorisation(*) or not? **Additional consideration** – prisoners rights / legal privilege issues.

Bibliography

A Review of Remote Surveillance Technology Along U.S. Land Borders, U.S. Department of Homeland Security, Office of Inspector General, December 2005.

Ale B., *Risk, an introduction*, Routledge, London, 2009.

Cameron I, Raman, R., *Process systems risk management*, Elsevier academic press, Amsterdam, 2005.

CDC MMWR, *Guidelines for Evaluating Surveillance Systems*, May 1988 & *Updated Guidelines for Evaluating Public Health Surveillance Systems,* July 2001.

Dorn, Dr. A. Walter, *Tools of the Trade? Monitoring and Surveillance Technologies in UN Peacekeeping,* External Study, September 2007.

FEMA, *Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings,* 2005.

FEMA, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, FEMA-426/BIPS-06, edition 2, 2011.

Foust, Joshua and Ashley S. Boyle, "The Strategic Context of Lethal Drones," *American Security Project*, 16 August 2012.

Foust, Joshua, "Yes, Sometimes Drones are Actually Effective," *The Atlantic,* 24 July 2012, http://www.theatlantic.com/international/archive/2012/07/yes-sometimes-drones-are-actually-effective/260260/, 6 March 2013.

Gill M. & Spriggs A., *Assessing the Impact of CCTV*. Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate, 2005.

Heinrich H., *Industrial accident prevention*, 3rd ed. McGraw Hill Book Company New York, Toronto & London, 1950.

La Vigne, Nancy G, Samantha S. Lowry, Joshua A. Markman, and Allison M. Dwyer, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention*, Community Oriented Policing Services (COPS), U.S. Department of Justice and The Urban Institute, September 2011.

Lingel, S., Menthe, L. Alkire, B., Gibson, J., Grossman, S.A., Guffrey, R.A., Henry, K., Millard, L.D., Mouton, C.A., Nacouzi, G. & Wu, E., *Methodologies for Analyzing Remotely Piloted Aircraft in Future Roles and Missions*, RAND, 2012.

Matarrese, Andy, "U.S. official defends drone strikes as legal, effective," *UPI.com*, 1 May 2012. http://www.upi.com/Top_News/Special/2012/05/01/US-official-defends-drone-strikes-as-legal-effective/UPI-56721335894649/
6 March 2013.

NEN-ISO 31.000 *Risk Management – Principles and guidelines* (ISO 31000: 2009, IDT)

RAND, *Methodologies for Analyzing Remotely Piloted Aircraft in Future Roles and Missions*, 2012.

Rios-Caberera R, Tuytelaars T. & Van Gool L., "Efficient multi-camera vehicle detection, tracking and identification in a tunnel surveillance application," *Computer vision and image understanding* 116: 742, 2012.

Roland HE & Moriarty B., *System safety engineering and management* 2nd ed., John Wiley & Sons, New York, 1990.

Safety Management Manual, ICAO document 9859 AN/490, 2006.

Schlosberg, Mark and Nicole A. Ozer, *Under the Watchful Eye*, The California ACLU Affiliates, August 2007.

Thayer RH, Fairly RE & Bjorke P., *IEEE Guide for information technology – System definition – Concept of Operations (ConOps) document*, IEEE Std 1362-1998, 1998.