SIAM

Security Impact Assessment Measures

Work package 3: Impact analysis on criminal actions

Deliverable 3.3 – Local Security Technology Effectiveness report

Massimo Migliorini

Roberta Sabbatelli

Sabrina Ricauda

Work package 3

Impact analysis on criminal actions – Deliverable 3.3

Project number

Call (part) identifier

Funding scheme

Table of Content

INTRODUCTION & EXECUTIVE SUMMARY

The following document describes the results of the work done by SITI within SIAM Project, Work Package 3.

The objective of WP3 is to evaluate the well established as well as failed impact that SMTs had on criminal actions. WP3 aims at answering how far SMTs are able to prevent or at least to disturb criminal actions.

The document is structured in 5 sections:

1. **Objectives:** the section states the objectives of the report.
2. **Methods**: the section describes the methods used for data collecting and reporting.
3. **Findings:** the section describes the main findings, with particular focus on the inter-relations between criminal actions and SMTs and crime mitigation mechanisms.
4. **Conclusion:** the section provides a conclusion based on the research findings.
5. **Annex:** the section provides an annex with tables listing, for each SMT, assessment criteria that are being used to assess the impact of SMTs (e.g. effective detection, organisational impact and increase in efficiency) and attributes that are being used to operationalize them.

1. OBJECTIVES

The primary objective of WP3 is to define a cluster of most frequent/most dangerous criminal actions, and to relate them to different Technologies Typologies defined in SIAM Project (see deliverable D2.3) in order to evaluate how far SMTs have been able to prevent or at least disturb criminal actions. WP3 wants to capture in particular *how* the SMTs are able to deal with identified criminal actions, that is which crime mitigation mechanisms different SMTs are able to provide. Last but not Least, WP3 aims at deriving a cluster of assessment criteria, attributes and questions for SIAM AST (Assessment Support Tool).

2. METHODS

Data were collected through interviews to experts. It was decided to perform interviews instead of a workshop because of two issues: on the one hand, we found that one-to-one interviews are able to create a more confidential relationship with experts, allowing them to feel more comfortable and thus share "more" information; on the other hand, the possibility to choose different dates for different experts allowed us to perform a higher number of interviews.

The following competencies and expertise were involved during the interviews:

- Criminology and Criminal patterns
- Security Systems for indoor environments
- Protection of citizens' Privacy
- Information and Communication Security Systems
- Security and Safety in work environment
- Mass Transport Security Systems
- Security Control & Monitoring Systems

Questionnaires were submitted to experts during the interviews, based on SIAM WP3 Official Guidelines. The questionnaires aimed at understanding three main points:

a) Frequent and dangerous criminal actions
b) SMTs
c) SMTs Impacts on criminal actions

Gathered information were elaborated and divided into 9 Technologies Typologies, according to the classification developed in SIAM project:

Threat Detection

- *Object and Material Assessment SMTs* (also: *Screening SMTs*) are used within security measures to search and assess people, luggage, cargo and airport deliveries to identify possible dangerous or illegal objects and substances e.g. weapons, drugs, or explosive residue.
- *Event Assessment SMTs* attempt to identify an unfolding crime by, for example, using CCTV to detect *suspicious behaviour* or to spot *abandoned luggage*.

- *People Assessment SMTs* are used in measures designed to identify potential malefactors. This includes questioning strategies, profiling methodologies such as background checks of passengers, or asymmetric screening based on demographics.

Access Control

- *Identification SMTs* are used to identify people as part of security measures designed to establish access rights.
- *Physical Access SMTs* relate to the broad category of physical barriers and access technologies such as turnstiles, perimeter fencing, and automated car park barriers.

Support

- *Process Control SMTs* capture the range of technologies that configure the security process, including the control of passenger flow, and the randomised or intentional selection of security measures applied to individual passengers.
- *Information and Communication SMTs* capture the computing and communication technologies used for a variety of different security measures within any security regime, such as those which can be found in devices and algorithms for information processing, as well as data transfer and storage.

Policing

- *Situation Awareness SMTs* includes the use of CCTV (increasingly employing PTZ cameras) to monitor an environment and liaise with staff on the ground, and the use of asset management solutions such as RFID tags and readers to track baggage and passenger movements or ANPR technology to identify vehicles.
- *Enforcement SMTs* are technologies used in security measures that respond to some process deviations or detected threats, such as those ensuring that each piece of hand luggage is screened or those dealing with weapons detection.

3. FINDINGS

2.1 Frequent and dangerous criminal actions

What are the most frequent criminal actions?

- Illicit physical access (with locks breaking/sabotaging)
- Objects/equipment theft
- armed robbery
- physical/psychological violence, shouting
- vandalism
- pickpocketing
- credit card cloning
- hacker attacks
- identity stealing
- data falsification

Why do they occur frequently?

The high frequency of these actions is due to a series of reasons:

a) **Low security level/absence of surveillance**: these criminal actions are frequently carried out in places easily reachable and not adequately protected. Security is often ignored and in most cases security systems are installed only after the criminal action was committed or in case of a major event. By the way, the problem of not monitored accesses can cause serious issues also from a safety point of view. In fact, "if an accident occurs so that a company has to be evacuated, and a guest or an external co-operator is inside without having being registered, security operators don't know exactly how many people have to be put in a safe area, engaging the risk to forget someone".

b) Easiness to be performed: normally these criminal actions do not require specific competences or expertise, nor involve particularly invasive activities. The "easiness" to perform such crimes is one of the most relevant causes of their high frequency.

c) **High possibility to hide crime evidences:** even if in some cases (pickpocketing, illicit physical access) it is quite difficult to hide clues, most of the mentioned criminal actions (in particular hacker attacks, identity stealing, etc.) can be masked as security system failures. In some cases, it is quite easy also to confound security operators by masking the "source" of the attack (for instance, performing multiple cyber-attacks from different ICT devices).

d) **Low cost:** a low economic effort is typically associated to these criminal actions. This aspect clearly increases their frequency.

e) **No special equipment needed:** these criminal actions are frequently carried out because they do not require hi-tech equipment (excluding some kinds of cyber-attacks) nor particular high-level training.

f) **Low possibility of be prevented/monitored/spotted:** from the security operators point of view, dealing with these criminal action is often very hard, also because the use of too heavy security measures may go against freedom of individuals. "SMTs are sometimes too complex and the privacy often causes a restriction for the security. It is necessary to find the right balance between privacy and security."

g) **Low consequences in case of proven guilty:** this aspect is mainly related to low-impact crimes, such as shouting, illicit physical access, etc. In some cases security operators prefer even not to take any measures and just "forget" the crime, after spotting it. There can be different reasons for this aspect: for example they might want to hide their negligence in performing their role, or they might feel, by their experience, that people involved are not so dangerous.

What are the most dangerous criminal actions?

- **Illegal use, illegal sale, and theft of CBRN agents** (Chemical, Biological, Radiological, and Nuclear). We are talking about nuclear and biological material therefore we are talking about difficult to source material. However, there are Countries that have resorted to the black market.

  An example can be the 1995 Tokyo subway Sarin gas attack (The Sarin attack on the Tokyo subway, usually referred to in the Japanese media as the Subway Sarin Incident, was an act of domestic terrorism perpetrated by members of Aum Shinrikyo on March 20, 1995. In five coordinated attacks, the perpetrators released Sarin on several lines of the Tokyo Metro, killing thirteen people, severely injuring fifty and causing temporary vision problems for nearly a thousand others. The attack was directed against trains passing through

Kasumigaseki and Nagatachō, home to the Japanese government. It is the most serious attack occurred in Japan since the end of World War II). This is an example on how CBRN weapons cause psychological terrorism, representing a very dangerous crime typology.

- **Security vulnerabilities created by insiders or ex-insiders** (ex. fired employees): "one of the heaviest crime action could be the incursion in a company of an outside person or a dissatisfied employee / dependent. More common would be the second case, since it is easier for someone knowing a factory to get into it and to cause heavy damages". Inadequate training procedures also represent a relevant cause of this kind of crime events.
- **Illicit physical access in very restricted security areas:** "Since the companies quite often have dangerous machineries, it is vital that only authorized personnel have access to certain areas." This criminal action seems to have less impact in case of small companies, due to the fact that employers better know each other. ("On our region, with mainly small companies, everyone knows everyone, therefore intrusion is easy to be fought or avoided).
- **Heavy vandalism** actions (e.g. security devices damaging).
- **Illegal access to confidential information**
- **Theft of crucial objects/security equipment**
- **Terrorist attacks** (bombs, Kamikaze, rifles)
- **Illegal goods smuggling**
- **Children or rare animals smuggling** ("it is true that normally people travelling with children are not terrorists, but they might be illicit traffickers of children").
- Any action that can cause temporary or permanent transport service interruption

What makes these actions dangerous?

a) **Possibility to have a big impact (mass panic, economic damage, huge money loss)**. The risk increases if the company is big and with a worldwide business.
b) **Possibility to have a huge impact in terms of loss of human lives.** CBRN /Terrorist attacks typically have the heaviest impacts in this sense.
c) **Possibility to increase security vulnerabilities in case of accidents: "**if an accident occurs so that the company has to be evacuated, and a guest or an external co-operator is in the factory without having being registered, we don't know exactly how many people have to be put in a safe area and the risk is to forget someone".
d) **Opportunity to favour money laundering and to fund organized crime** (drugs distribution, humans smuggling, etc.).

2.2 SMTs

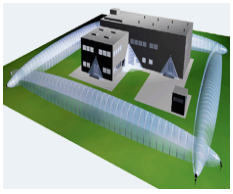
What kind of SMTs is being operated to deal with these criminal actions?
There is a wide number of SMTs able to deal with mentioned criminal actions:

Closed-circuit television cameras (CCTV) in internal and external areas.

(TYPE: Situation Awareness)

Metal detectors

(TYPE: Object and Material Assessment)



Active anti-intrusion systems with acoustic alarm, SMS or call alarm, etc. for internal areas. If we couple IR and microwave anti-intrusion systems there is an efficiency improvement and a false alarms limitation.

(TYPE: Event Assessment/Situation Awareness)

Two-factors recognition systems (e.g. Password and token)

(TYPE: Identification)

Biometrics (Face Recognition, Eyes recognition, etc.)
(TYPE: Identification)

Cyber-security Systems
(TYPE: Information and Communication)

Tail-Gating Preventions Systems

(TYPE: Physical Access)

Measures against CBRN attacks (TYPE: Object and Material Assessment)

As an example, on the International Atomic Energy Agency (IAEA) website there is a database where the Member States (about 100 on a voluntary basis) agree to report any illegal activity that may occur in their territory (e.g. Illegal nuclear traffic). Anyway, in the chemical-biological field, in case of a terrorist attack thread, Interpol is the body acting immediately to solve the emergency situation. Other important SMTs are represented by Security measures adopted inside CBRN laboratories. In this case we talk about prevention instead of detection. On the IAEA website there is a section where we can see

the statistics showing whether the illegal trade was detected through technology or through investigation. On the Monterey Institute website there is a similar database, which reports information about nuclear material illegal trade taken from newspapers.

Are there any major technological innovations that have been introduced? Are any technological innovations expected that will enhance the possibility to deal with them?

- Concerning CBRN, upgrading processes are continuously taking place for detection/prevention measures, but most of these information are classified. Some of most recent CBRN equipment innovation can be anyway found in private companies CBRN magazines.
- Anti-intrusion systems are quite a mature technology, thus no specific innovation are foreseen.
- An Innovative security system was recently been developed to limit the photovoltaic panels theft. The instrument consists of an optical fibre with an electric system that passes through all panels. If the panel is removed, the electric signal is interrupted and the system gives an alarm.
- Recent developments in CCTV sector include innovative audio/video analysis tools (object tracking, people profiling, behaviour recognition, etc.).
- Voice recognition systems and "Typing Keys" recognition system, associated to CCTV, seem to also be a promising path of research and development. ("CCTV systems need to be improved in their definition and their performance, e.g. zoom in details").

2.2 Impact of SMTs on criminal actions

In which way have the SMTs contributed to security, and are there different dimensions of security affected?

In general, it can be said that SMTs have a positive effect on criminal actions reduction, people feel more "secure" when they know that criminal actions frequency is low. Recording, Discovering, Detecting, Disturbing are example of crime reduction mechanisms contributing to this purpose. However, the use of an SMT clearly reflects on other dimensions too, like Privacy and Freedom Infringements. The debate about the roles of SMTs and their limits is heavily handled in other SIAM Work Packages therefore it will not be detailed here, but it is worth to say that SMTs limit is not a fixed threshold, but a variable boundary depending on several aspects such as SMTs type, people affected, cultural backgrounds, territorial contexts, local traditions, criminal actions taken into account, and even users subjective feelings/perceptions. There is a sort of contradictory perspective among SMTs Users: many people believe that recording a crime is a clever way to discover the identity of the criminal, but they do not want CCTV data to be recorded. As another example, many people are convinced that identity stealing is a high-impact criminal action, but they do not like that their data are stored in databases. It is thus quite difficult to understand which is the real balance between different Security dimensions and Freedom dimensions for SMTs. To solve these issues, in the Italian context, decision-makers typically use a "empirical approach": the use (and invasiveness) of SMTs is pushed forward up to the point that a relevant number of people complain about it. By the way, the huge recent diffusion of control and surveillance SMTs is someway accustoming people to be "controlled". The capability of Regulatory Systems to enforce a right use of SMTs (and to avoid

indiscriminate data dissemination) is also favouring these SMTs diffusion processes, giving people the sensation that their interests and privacy are someway protected exactly by the same mechanism that they perceive as a threat ("without rules there is no freedom, it is better to be checked and to be safer"). Media have also a great power in influencing global security notions and perception of SMTs. Even if more often they hinder instead of favouring SMTs diffusion, a positive effect can occur when media insist on a particular crime-case, evidencing specific security vulnerabilities and fostering people to adopt technological counter-measures.

What is the impact of SMTs on crime?
<u>There are several mechanisms among which SMTs may deal with criminal actions:</u>

a) Prevention: some SMTs are designed to make physically impossible performing criminal actions. This is the case for example of tail-gating prevention systems.
b) Dissuasion: CCTV is a clear example working with this mechanism, especially if associated to warning signs. Criminals are dissuaded to act since they are aware to be controlled, and/or they can be easily identified. This is also the case of Identification Technologies (biometrics).
c) Disturbing: "when is not possible to prevent a crime, it can be anyway disturbed during its performance". SMTs like sound alarms, light alarms, smoke diffusers are an example of SMTs using this mechanism, since they are able to slow down criminal action execution by altering criminals senses (sight, hearing, movement) and reducing the remaining time to achieve their criminal purposes (raising the attention of neighbours or calling police forces).
d) Consequence Mitigation: a criminal action is always done with a specific purpose. If that purpose is denied, than such criminal action will lose any appeal. Security protocols that are able to mitigate or even completely cancel the consequences of a cyber-attack (Emergency Back-up, Alternative Server Routing, Access blocking, etc.) act as a deterrence for such kind of criminal actions.
e) Spotting/Highlighting Crime Evidences: Even in case there is not any proven guilty, the awareness that a criminal action can potentially be committed raises people attention, acting as deterrence towards crimes performing. Metal detectors are a great example of a SMT using this principle. Anti-intrusion systems and respective sound/light alarms also use this mechanism to deal with illicit physical accesses.

It is important to highlight that SMTs themselves are not enough if people that are supposed to use them are not adequately trained. Training and information are fundamental. Mandatory tools must be: awareness, training, political support in the implementation of technology.

<u>How is the impact being assessed / measured?</u>
Some people think that often it is difficult to assess the impact of a SMT ("if nothing happens and everything works fine and in the correct way how can the impact be calculated?"). Despite of this statement, a series of factors that may help to measure SMTs impacts have been identified:

a) **Crime statistics:** crime reduction rating is a relevant indicator of SMTs effectiveness.
b) **Medias Feedback:** Medias play a relevant role in assessing technologies effectiveness, in particular TV news. If a criminal is caught thanks to a certain technology, it means that this technology works. A good feedback by Media represents undoubtedly a good indicator of SMTs effectiveness.

c) **Market Surveys & Sell statistics** also represent a potential indicator ("an easily sold SMT is most of the times an effective SMT").
d) **Cost-benefit ratio**: the impact of criminal actions on Turin metro system is measured through money spent to repair damages in comparison with the passengers number. If this number decreases after installing a SMT, usually the SMT is considered effective.
e) **Risk Assessments and Audit**, using both qualitative and quantitative methodologies can represent a way to assess SMTs effectiveness. Qualitative methodologies are based on security perception (interviews, surveys, social networks) while quantitative methodologies are based on crime events number and on associated money loss.

When is an SMT ineffective?

Usually an SMT is considered ineffective when it does not achieved the purpose it was designed for (preventing, disturbing, mitigating crime actions), or it does not even reach an established minimum threshold of efficiency.

It is not considered effective also when it is rejected / untrusted by users, or if it involves relevant ethics issues (ex: freedom infringement, privacy, discrimination).

A relevant impact on its perceived effectiveness comes also from the possibility to be "regulated" (in terms of laws) and "used" (in terms of training requirements for security operators and constraints / enforcements for users). Problems may occur also if the SMT is not associated to adequate communication procedures, and it can be easily used for other purposes such as market-surveys or illicit data traffic. ("For the video surveillance a bad use would be not to inform people that they are being recorded or, even worse, to put cameras in places such as dressing rooms in stores").

Some SMTs (like Anti-intrusion systems) are considered ineffective when they are not able to reduce false alarms or when they take a significant amount of time to call police forces.

Clearly, false alarms rate and failure rate represent as well two important indicators of SMTS ineffectiveness.

How do notions of crime and security change in the course of the introduction of SMTs?

Some people think that notions on crime and security will never change at all. Others believe that crime notions follow technology evolution, in particular in the case of cyber-crimes (reminding virus-antivirus dynamics). The globalization is also believed to play a relevant role in influencing security and crime notions at European level: a wider communication paves the way to best practices comparison and security approaches sharing, but unfortunately it also fosters crime techniques diffusion. As people today travel more and for longer distances along different Countries, the lack of a unique security concept and the gap between different countries (or even transport systems) in terms of security approaches and procedures represents a great challenge Europe is going to deal with in the next future.

The recent trend about security perception (e.g. more and more increasing awareness on security issues, as well as more diffused knowledge on security systems) also plays a significant role in security notions evolution within current and future societies.

In the future it is foreseen that the global perspective of security, with particular reference to privacy issues, will probably change. Today Privacy is seen as an obstacle to technologies use and in some

case to global security. But this perspective is changing, and Privacy is more and more seen not as "less security systems, but as more clarity on their use".

Which unintended consequences have been observed after the implementation of the specific SMT?

One of the most common unintended consequences of SMTs is typically the rejection by users, usually due to freedom infringements or trust/acceptance issues. ("Some security rules applied in certain airports are annoying, such as questionnaires to be filled in when you enter a certain country. These questionnaires are a pure formality and a waste of time.").

Some SMTs are in fact perceived as too invasive, or even too dangerous for human health (like Body Scanners).

Some SMTs instead resulted being much less effective than foreseen. ("If you think about the disasters that have hit mankind during these last few years (Twin towers and Madrid station), you agree in saying that technology can really deceive. Both places had security systems and up-to-date technology, but they weren't effective").

CCTVs in particular had unintended consequences on inhabitants privacy and in their organizational routine (e.g. monitored street during the night are more populated compared to not monitored streets). While some of these unintended consequences may be really positive (in Turin Metro for instance travellers security perception in metro internal area is improved after the implementation of CCTV control systems), in other cases some negative issues may arise ("Security forces think that CCTVs are able to substitute them for everything but it isn't true"). Anti-intrusion systems typically do not show specific unintended consequences, except of potential false alarms.

To what extent have the promises of SMTs been delivered?

Different opinions on this subject were collected:

- Generally speaking, when creating a new technology, if all rules and procedures are respected, this technology will do what it has been made for. "Let's take the Twin Towers as a case. The controllers hadn't done scrupulous checks. If the existing rules had been applied the terrorist attack would not have happened. Also the Intelligence didn't do what it was expected. Nowadays in some critical airports, the controls have been implemented also to raise awareness on security among people".
- SMTs make criminal actions more difficult to be realized, but not impossible. ("If you wish, anything could be eluded. Rules are created after a crime has been committed").
- Concerning more mature SMTs (such as CCTV systems and Anti Intrusion Systems), expectations were respected but there are always more and more requirements to face most recent crime actions, thus as a consequence SMTs are continuously changing.

4. CONCLUSION

In general, it can be said that SMTs have a positive effect on criminal actions reduction, people feel more "secure" when they know that criminal actions frequency is low. Recording, Discovering, Detecting, Disturbing are example of mechanisms contributing to this purpose. However, the use of an SMT clearly reflects on other dimensions too, like Privacy and Freedom Infringements. It is worth to say that SMTs limit is not a fixed threshold, but a variable boundary depending on several aspects such as SMTs type, people affected, cultural backgrounds, territorial contexts, local traditions, criminal action taken into account, and even users subjective feelings/perceptions. It is thus quite difficult to understand which could be the right balance between different Security dimensions and Freedom dimensions for SMTs.

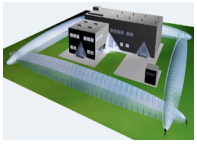
It is interesting to have an overview on different people feelings towards both crime actions and security notions. Some people think that notions on crime and security will never change at all. Others believe crime notions follow technology evolution, in particular in the case of cyber-crimes (reminding virus-antivirus dynamics). The globalization is also believed to play a relevant role in influencing security and crime notions at European level: a wider communication paves the way to best practices comparison and security approaches sharing, but unfortunately it also fosters crime techniques diffusion. As people today travel more, and for longer distances along different Countries, the lack of a unique security concept and the gap between different countries (or even transport systems) in terms of security approaches and procedures represents a great challenge Europe is going to deal with in the next future.

It is worth to highlight also that in the future the global perspective of security, with particular reference to privacy issues, will probably change. Today Privacy is seen as an obstacle to technologies use and in some case to global security. But this perspective is changing, and Privacy is more and more seen not as "less security systems", but as "more clarity on their use".

5. ANNEX

The following tables list for each SMT, the assessment criteria that are being used to assess the impact of SMTs (e.g. effective detection, organisational impact and increase in efficiency) and the attributes that are being used to operationalize them.

SMT Type	Crime/Threat	Assessment Criteria	Attribute
CCTV (TYPE: Situation awareness) 	Theft in the public terminal area	Prevention Dissuasion	Crime reduction rate Impacts reduction rate (social)

SMT Type	Crime/Threat	Assessment Criteria	Attribute
Metal detectors (TYPE: Object and Material Assessment) 	- Armed robbery - Vandalism - Illicit physical access (with locks breaking/sabotaging) - Illegal use, illegal sale, and theft of CBRN agents - Security vulnerabilities created by insiders or ex-insiders - Illegal access to confidential information - Terrorist attacks - Illegal goods smuggling - Children or rare animals smuggling	Spotting/Highlighting Crime Evidences	Crime reduction rate Impacts reduction rate (casualties) Impacts reduction rate (economics) Impacts reduction rate (social)
Active anti-intrusion systems (TYPE: Event Assessment/ Situation Awareness) 	- Illicit physical access (with locks breaking/sabotaging) - Theft - Armed robbery - Physical/psychological violence , shouting - Vandalism - Terrorist attacks	Prevention Disturbing Spotting/Highlighting Crime Evidences	Crime reduction rate Impacts reduction rate (economics) Impacts reduction rate (social)
Two-factors recognition systems (TYPE: Identification) 	- Illicit physical access (with locks breaking/sabotaging) - Credit card cloning - Hacker attacks - Identity stealing - Data falsification - Security vulnerabilities created by insiders or ex-insiders - Illegal access to confidential information	Prevention	Crime reduction rate Impacts reduction rate (casualties) Impacts reduction rate (economics) Impacts reduction rate (social)

SMT Type	Crime/Threat	Assessment Criteria	Attribute
Biometrics (TYPE: Identification) 	- Identity stealing - Data falsification - Security vulnerabilities created by insiders or ex-insiders - Illegal access to confidential information	Prevention	Crime reduction rate Impacts reduction rate (economics) Impacts reduction rate (social)
Cyber-security Systems (TYPE: Information and Communication) 	- Credit card cloning - Hacker attacks - Identity stealing - Data falsification - Illegal use, illegal sale, and theft of CBRN agents - Illegal access to confidential information - Illegal goods smuggling - Children or rare animals smuggling	Prevention Disturbing Consequence Mitigation Spotting/Highlighting Crime Evidences	Crime reduction rate Impacts reduction rate (economics) Impacts reduction rate (social)
Tail-Gating Preventions Systems (TYPE: Physical Access) 	- Illicit physical access (with locks breaking/sabotaging)	Prevention Dissuasion Disturbing Spotting/Highlighting Crime Evidences	Crime reduction rate
Measures against CBRN attacks (TYPE: Object and Material Assessment) 	- Illegal use, illegal sale, and theft of CBRN agents - Terrorist attacks - Illegal goods smuggling	Prevention Dissuasion Disturbing Consequence Mitigation Spotting/Highlighting Crime Evidences	Crime reduction rate Impacts reduction rate (casualties) Impacts reduction rate (economics) Impacts reduction rate (social) Impacts reduction rate (environmental)