# A Dynamic Risk Assessment (DRA) Methodology for High Impact Low Probability (HILP) Security Risks

**Abstract.** This paper proposes Dynamic Risk Assessment (DRA) methodology applicable to the so-called High Impact Low Probability (HILP) threats which, by their very nature, are difficult to identify or occur only infrequently. DRA is based on the detection and processing of available Weak Signals (WSs) to protect critical infrastructures and soft targets against HILP security threats before they materialise. The proposed methodology allows to rank WSs according to the reliability and credibility of the sources and, to correlate them to obtain threat precursors. Experimental results have shown that DRA is effective and helps distinguish irrelevant alerts, thereby reporting significant threats to operators.

**Keywords:** Dynamic Risk Assessment, Low Probability High Impact risks, Security.

## 1 Introduction

This paper proposes a methodology to dynamically assess risks for the so-called High Impact Low Probability (HILP) threats which, by their very nature, are either difficult to identify or occur only infrequently [1]: in HILP category fall, in particular, terrorism, extremism, and lone wolf actions risks. The dynamic assessment of risks is an essential element of any decision support tool aimed at improving the situational awareness while protecting critical infrastructures and/or soft targets (e.g. mass gathering events) against HILP risks.

The proposed Dynamic Risk Assessment (DRA) approach is inspired by Intrusion Detection Systems approaches [2] and based on the detection and processing of Weak Signals[1] (WSs) collected from heterogeneous sources. WSs, once detected and correlated with other WSs, can generate precursor alerts of terrorism actions to be deeper and further investigated. The paper is organised as follows: Section 2 discusses the DRA approach, Section 3 proposes an example of the application of DRA to a mass gathering event and finally Section 4 presents conclusions and future work.

## 2 The proposed DRA approach

The proposed DRA approach bases its reasoning on the collection and processing of WSs, the minimum quantum of information managed by the DRA.

---

[1] A WS can be defined as "*A seemingly random or disconnected piece of information that at first appears to be background noise but can be recognized as part of a significant pattern by viewing it through a different frame or connecting it with other pieces of information*" [11]

On the basis of the proposed WS definition, the logic behind DRA can be summarised in the following steps:

1. **Collect** the WSs from heterogeneous sources;
2. **Analyse** each collected WSs and verify if, alone or correlated with other existing WS, can represent a more **significant precursor** of a threat and present it to a security operator for evaluation;
3. **Re-assess the risks** for the crowd accordingly.

In the following each step of the methodology is described in more detail.

### 2.1 The WS collection

Each WS, detected by a given source, contains the following minimal information:

- A unique **ID** that has embedded the reference to source of the WS;
- The absolute time **t** in which it has been collected;
- The **geolocation** (x, y) - if available;
- A **snapshot** of what has been detected using a pre-defined semantic (e.g. using keywords) to help the operator to confirm, discard (false or nuisance alarms) or amend the detection of the source.

Each detected Weak Signal is characterised by a **Significance** (**S**) value assigned to it that is a combination of:

- The **Reliability** (**R**) of the source, that characterises the source independently from the considered item of information;
- The **Credibility** (**C**) of the source, that introduces a measure of the degree of confirmation: the more an item of information is confirmed, the higher its credibility and, conversely, the more an item of information is contradicted by others, the less credible it becomes [3].

The Significance of the considered WS detected by the source *m* ranges in the [0, 1] interval and is computed as follows:

$$S(WS_{ID}) = (\alpha \cdot R_m + \beta \cdot C_m) / NF \quad (1)$$

where:

- C and R are integer in [0, 5] (where 1 is very low and 5 is very high);
- The Normalising Factor NF keep $S(WS_{ID})$ in [0, 1];
- $\alpha$ and $\beta$ are correcting factors to tune the role of each factor in the product.

If the proposed methodology is applied to an event (e.g. a concert in a stadium) it is possible to add a further element that consider the Time Distance ($TD_t$) from the event venue: the closer the event venue the greater the $TD_t$ value. $S(WS_{ID})$ then becomes:

$$S(WS_{ID}) = (\alpha \cdot R_m + \beta \cdot C_m + \gamma \cdot TD_t) / NF \quad (2)$$

### 2.2 WS processing and Suspicious Signs/Patterns generation

Once received, it is necessary to process WSs to evaluate if they can become, alone or in together with other WSs, a **significant precursor** of a threat and to distinguish irrelevant alerts, thereby reporting significant threats only. To this end three structures of **Precursors** are introduced:

- **Suspicious Sign** (**SS**), represents a single WS that has either sufficient significance to become a SS or is related to high-risk threat. In both cases, S(SS) = S(WS).
- **Intelligence Alerts** (**IA**), i.e. those WS coming from the intelligence services, can be considered a special Suspicious Event with maximum Significance S(IA) = 1;
- **Suspicious Pattern** (**SP**), two or more WSs can create a SP if they have sufficient significance and are linked together according to one of the criteria described below.

The Precursors can be generated combining already collected WSs, SSs, IAs or SPs:

1. Statically, using the **experts' knowledge** to define the rules for grouping WSs;
2. Dynamically, using an automatic grouping of WS using logic similar to those currently used, for example, at some airport security checks: 3 or more credible WS "**simultaneously**" (i.e. within a short period of time) coming from different sources of information can be considered as SP;
3. Using **data analytics** on received WS e.g. using deep learning techniques [4] [5] [6].

Therefore, Precursors can be of 7 types:

- **Group**: a set of WS/SS/SP without time and geographic constraints independently of the time sequence in which they are detected;
- **Sequence**: a set of WS/SS/SP that need to be received in the correct sequence.
- **Area**: a set of WS/SS/SP within the same area and in a given time interval;
- **Distance from Hot Spots**: a set of WS/SS/SP in a given time interval all at a distance from Hot Spots shorter than a given threshold;
- **Simultaneous Group**: the grouping is generated using the strategy of "**simultaneous events**" described in point 2. above;
- **Data Analytics**: the grouping of WS/SS/SP is generated using **data analytics** approaches for example through the generation of new rules on the basis of data collected in the past. A possible approach is described in [7], where Suspicious Activity Reports (SAR) collected by 911 emergency operators are analysed to identify and prioritise cases of interest from the large volume of SARs;
- **Operators Group**: the grouping of WS/SS/SP is generated by the operator according to his/her experience.

Precursors' Significance value is computed using the Significance values of all the WSs connected to it. The approach to combine Significance values for an SP with 2 elements contributing to it with significance $S_1$ and $S_2$ respectively, is derived from Certainty Factors [8] theory using the following formula

$$S_{1\ and\ 2} = S_1 + (1 - S_1) \cdot S_2 \tag{3}$$

Having more than 2 elements contributing to the same SP, it is possible to iteratively apply the same formula (in case of 3 elements with $S_1$, $S_2$ and $S_3$, respectively):

$$S_{1\ and\ 2\ and\ 3} = S_{1\ and\ 2} + (1 - S_{1\ and\ 2}) \cdot S_3 \quad (4)$$

### 2.3 Dynamic re-assessment of risk

Precursors, when triggered by WSs, can be then classified as:

- **Non-Critical**, i.e. elements that do not constitute an immediate threat;
- **Critical**, i.e. elements that constitute an immediate threat.

**Critical Precursors** shall be triggered and brought immediately to the attention of a security operator that should take the necessary mitigation actions.
Using the above methodology, the **Risk Level** can be re-assessed using escalation approaches [9]. An example, when dealing with a mass gathering event, based on an IF-THEN-ELSE approach is given in the following:

- IF (Time Distance from the event is Far) AND (no Critical SS or SP are triggered) THEN (the Risk Level is Very Low);
- IF (Time Distance from the event is Far) AND (some Non-Critical SS or SP are triggered) THEN (the Risk Level is Low);
- IF (Time Distance from the event is Far) AND (at least one Critical SS or SP is triggered) AND (Crowd Density is Low) THEN (the Risk Level is Medium);
- IF (Time Distance from the event is Close) AND (at least one Critical SS or SP is triggered) AND (Crowd Density is Low) THEN the Risk Level is High;
- IF (Time Distance from the event is Close) AND (at least one Critical SS or SP is triggered) AND (Crowd Density is High) THEN the Risk Level is Very High.

Clearly, exact IF-THEN rules and thresholds need to be defined according to laws, protocols and best practices including also socio-political and environmental conditions.

## 3 The DRA application to a mass gathering event: an example

### 3.1 The DRA practical implementation

DRA methodology has been applied to a scenario representing a mass gathering event managed by a Law Enforcement Agency (LEA). The sources of WSs are:

- Normal citizens calling 112 emergency services;
- Stewards recruited to manage the event;
- CCTV-based video-processing tools (HCCV) able to (semi-)automatically recognise car plates, identify vehicles and suspicious behaviours of vehicles and individuals;
- Intelligence services.

The sequence of WS detection, SP generation and dynamic risk assessment is described in **Fig. 1**:

1. On the basis of the received WS, the corresponding values of sensor's credibility and reliability and the time distance from the event are identified.
2. The Significance is then computed using the formulas in Section 2 (with $\alpha$, $\beta$ and $\gamma$ set to 1 for the sake of simplicity) and normalised to get values in the [0; 1] range.

**Fig. 1.** DRA applied to a mass gathering event

| Time | Signal/Pattern | Sensor | Description | Reliability R | TD | Significance | Norm. Significance | Alert Level |
|---|---|---|---|---|---|---|---|---|
| T01 | WS01 | Citizen | Suspicious Vehicle | 4 | 1 | 8 | 0,06 | |
| T02 | | | | | | | | |
| T03 | WS02 | HCCV | Suspicious Behaviour | 3 | 1 | 6 | 0,05 | |
| T04 | WS03 | Citizen | Suspicious Vehicle | 4 | 1 | 8 | 0,06 | |
| T05 | **SP01** | DRA Rule | Suspicious Vehicle | **WS01 & WS02 & WS03** | | | 0,17 | |
| T06 | Patrol sent to check | | | | | | | |
| T07 | SP01 deleted after operator's check | | | | | | | 1 |
| T08 | IA01 | Intelligence | Possible terrorist attack | 5 | 2 | 50 | 0,40 | 3 |
| T09 | WS04 | HCCV | Red truck | 5 | 2 | 40 | 0,32 | |
| T10 | IA02 | Intelligence | Stolen yellow van | 5 | 2 | 50 | 0,40 | |
| T11 | WS05 | HCCV | Suspicious plate detected | 5 | 2 | 50 | 0,40 | |
| T12 | **SP02** | DRA Rule | Suspicious Vehicle | **IA02 & WS05** | | | 0,64 | |
| T13 | IA03 | Intelligence | Terrorist presence | 5 | 3 | 75 | 0,60 | |
| T14 | Reaction due to IA03 | | | | | | | |
| T15 | WS06 | HCCV | Brown truck | 5 | 3 | 60 | 0,48 | |
| T16 | WS07 | HCCV | Red van | 5 | 3 | 60 | 0,48 | |
| T17 | WS08 | HCCV | Suspicious plate detected | 5 | 3 | 75 | 0,60 | |
| T18 | WS09 | HCCV | Blue car | 5 | 3 | 60 | 0,48 | |
| T19 | WS10 | HCCV | Suspicious plate detected | 5 | 3 | 75 | 0,60 | |
| T20 | WS11 | Steward | Suspicious person | 5 | 3 | 75 | 0,60 | |
| T21 | WS12 | HCCV | Suspicious plate detected | 5 | 3 | 75 | 0,60 | |
| T22 | **SP03** | DRA Rule | Suspicious Vehicle | **WS08 & WS10 & WS12** | | | 0,94 | |
| T23 | Reaction due to SP03 | | | | | | | |
| T24 | WS13 | Steward | Suspicious person | 5 | 3 | 75 | 0,60 | |
| T25 | **SP04** | DRA Rule | Probing security | **WS11 & WS 13** | | | 0,84 | 4 |
| T26 | WS14 | HCCV | Quite dense crowd | 4 | 5 | 80 | 0,64 | |
| T27 | WS15 | HCCV | Yellow van | 5 | 5 | 100 | 0,80 | |
| T28 | **SP05** | DRA Rule | Ramming vehicle | **SP02 & WS15** | | | 0,93 | 5 |
| T29 | Reaction due to SP05 | | | | | | | |

Through the application of the DRA rules the Precursors are created and, if necessary, Alert Level is modified.

First experimental results have confirmed the validity of the approach, as confirmed by the involved LEAs and that DRA helps distinguish irrelevant alerts, thereby reporting only significant threats to operators.

### 3.2 A possible architectural approach for DRA implementation

DRA decision support tool has been implemented to manage mass gathering events in a Web-server GIS-based architecture receiving WSs from a series of external tools generating using REST technology:

- Estimation of crowd density and sudden density changes from video streams;
- Estimation of crowd anomalous behaviours;
- Web crawling and semantic intelligence to detect suspicious messages;
- Crowd behaviour modelling to estimate consequences

SPs above a selected Significance threshold are brought to the attention of an operator to allow a risk-aware decision-making process with person-in-the-loop.

## 4 Conclusions

As reported in Section 3, experimental results have shown that DRA is effective and helps distinguish irrelevant alerts.

The proposed DRA methodology has the following advantages over more traditional approaches:

- It searches for **out-of-the-ordinary behaviours** and unseen threats;
- It allows **memory of hypotheses** and data rejected by security analysts and notices what **analysts are watching and asking**.

Moreover, the proposed DRA approach is fully in line with the European Security Model [10] that prescribes *"... stronger focus on the **prevention of criminal acts** and terrorist attacks before they take place can help reduce the consequent human or psychological damage, which is often irreparable*".

Finally, the DRA approach described in this paper is going to be further validated on real scenarios from Law Enforcement Agencies (LEAs).

### References


1. UK Government Office for Science, "Blackett Review of High Impact Low Probability Risks," London, 2011.
2. E. Chakir, M. Moughit and Y. Khamlichi, "A Real-Time Risk Assessment Model for Intrusion Detection Systems," in *2017 IEEE International Symposium on Networks, Computers and Communications (ISNCC)*, 2017.
3. North Atlantic Treaty Organization (NATO) Information Handling Services, "Annex to STANAG 2022 (Edition 8)," 1992.
4. H. Vu, "Deep Abnormality Detection in Video Data," Melbourne, 2017.
5. D. Xu, E. Ricci, Y. Yan, J. Song and N. Sebe, "Learning deep representations of appearance and motion for anomalous event detection," 2015.
6. M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury and L. S. Davis, "Learning temporal regularity in video sequences," Las Vegas, 2016.
7. K. J. Strom and J. P. M. Hollywood, "Using 911 Calls to Detect Terrorism Threats," June 2009. [Online]. Available: https://www.nij.gov/journals/263/pages/911-calls.aspx.
8. P. J. F. Lucas, "Certainty-factor-like structures in Bayesian belief networs," *Knowledge-Based Systems,* vol. 14, 2001.
9. UK HM Treasury , " Orange Book: Management of risk - Principles and Concepts," London, 2004.
10. Council of the European Union, *Internal security strategy for the European Union - Towards a European Security Model,* General Secretariat of the European Council, 2010.
11. P. J. H. Schoemaker and G. S. Day, "How to Make Sense of Weak Signals," *MIT Sloan Management Review,* vol. 50, no. 3, 2009.