Intelligent Human Systems Integration (IHSI 2023), Vol. 69, 2023, 312–318
https://doi.org/10.54941/ahfe1002850

A Framework for Hybrid Risk Analysis

Maryna Zharikova[1,2] and Stefan Wolfgang Pickl[1]

[1]Bundeswehr University Munich, Neubiberg, Germany
[2]Kherson National Technical University, Kherson, Ukraine

ABSTRACT

Changes within the worldwide security environment proceed to challenge our ability to comprehend and react to the constantly changing hybrid threats that are becoming more diverse, emanating from a wide range of actors who are enabled by technology. Actors can wield an array of means and ways to further their security interests at the expense of a target and are able to do so without being identified. Developing proper situational awareness is the first and crucial step on the road to achieving better protection against hybrid threats. Here we propose a novel framework for hybrid risk analysis that enables a better understanding of the operations of the adversary before their taking place. The idea of the framework is based on the model of hybrid operations, which combines the elements of space, time, objects at risk, goals, and actors into a single structure - a hyper-forest of multi-trees. Taking into account that hybrid operations are carried out according to certain scenarios characterized by the repeatability of tools in relation to certain goals, we propose using a case-based reasoning approach based on calculating the dynamic similarity of the information structure of ongoing attack to retrospective sequences of hybrid attacks for which the goals, tools, and methods are known. Retrospective data is stored in the case base. The proposed framework combines several models and methods, the main of which are the multi-tree model of hybrid attack representation, the spatially-distributed model of hybrid attack distribution, and the method for hybrid risk analysis. The method for hybrid risk analysis is based on two additional models such as vulnerability model and the consequences assessment model that are developed for each type of object at risk. The suggested framework for hybrid risk analysis offers a better comprehension of adversary operations prior to them occurring and aids in formulating an appropriate reaction to the changing scenario.

Keywords: Hybrid attack, Hybrid operation, Hybrid risk

INTRODUCTION

Changes within the worldwide security environment proceed to challenge our ability to comprehend and react to the constantly changing threat picture. (Hansen, 2021).

Threats to national security are becoming more diverse, emanating from a wide range of actors who can wield an array of tools to further their security interests at the expense of a target, and are able to do so without being identified (Hansen, 2021). Combining threats of different natures leads to the concept of hybrid threats.

The EU and NATO have made combating hybrid threats a top priority. About 20 of their proposals deal with this problem (Zandee, 2021). The EU's new strategic agenda for 2019–2024, explicitly considers resilience, hybrid threats, and misinformation to provide a strong mandate for the EU's future work (European Council, 2019). According to the agenda, the EU's top priorities in the area of protecting individuals and freedoms are enhancing the EU's resilience to both natural and man-made disasters and defending our society from damaging cyber activities, hybrid threats, and other security problems (Bajarūnas, 2020).

The European Union invests in projects which seek to strengthen the European Union's capacity and deal more efficiently with hybrid threats (European Union, 2022a).

Among the projects funded by the EU's framework programs for research and innovation, there are many projects dedicated to cybersecurity such as CYBER-PDR (Disempowering Cyber-Attackers) (2020–2021) (European Union, 2022b), NeCS (European Network for Cyber-security) (2015–2019) (European Network for Cyber-security, 2019), CONCORDIA (a Cybersecurity Competence for Research and Innovation) (2019–2022), CyberSec4Europe (Cyber Security for Europe) (Cyber Security Network of Competence Centres for Europe, 2019), PRAETORIAN (Protection of critical infrastructures from advanced combined cyber and physical threats) (2021–2023). It should also be mentioned the ongoing project EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) (2020–2025). EU-HYBNET is a Pan-European network that brings together security experts, stakeholders, academics, businesspeople, and SME actors from all around the EU to work together to combat hybrid threats (Diego, 2022).

Despite the fact that a lot of regulations and significant actions have already been made to increase Europe's resistance to hybrid threats, there is still much to be done in practice at the EU level. Many of the projects develop a set of regulations or rules, but in practical systems, there is a need for universal approaches that support decision-making at the stages of prevention, elimination, and mitigation of hybrid threats (Zandee, 2021).

PROBLEM STATEMENT

Attackers try to achieve a given strategic goal by attacking different domains in different ways using sequences of hybrid attacks (HAs). We assume that a hybrid operation corresponds to a certain series of HAs.

HAs are usually implicitly connected in time and location, which opens an opportunity to identify their connections by targets, domains, and goals. Besides, we assume that hybrid operations are quite repetitive with respect to their methods and goals, so we propose to use a case-based approach to assess hybrid threats.

We consider hybrid attacks as a kind of threat where the attacker blends two or more kinds of tools (such as the spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage) to achieve

a malicious goal. Hybrid attacks threaten targeted objects (bridges, railways, buildings, etc.) (Giannopoulos, 2021).

Hybrid operations are well-developed scenarios for the successive or even parallel use of hybrid attacks of a different nature on various objects using a wide range of tools, but with a common goal.

The main contribution of this work is to deliver a novel framework for hybrid risk analysis. The novelty of this work in comparison with the related ones is that the proposed framework covers three main stages of the decision-making process such as prevention, response, and post-crisis.

What is also novel is that the risk is divided into potential (for the prevention stage), active (for the response stage), and post-crisis risk (for the post-crisis stage), which allows decision-makers to make more informed decisions at every stage of the decision-making process.

HYBRID ATTACK MODEL

Hybrid attack (HA) HA_{ij} is carried out by a certain actor A_i and is directed at a certain vulnerable object O_j at a certain point in time t.

Each actor A_i has a set of tools T_i to carry out HA. The set of tools can change over time: $A_i = \{T_i(t)\}$. Let's introduce the notion of an actor's state, which depends on a set of tools available to him. To determine the state of the actor A_i, we introduce a qualitative scale that reflects the danger of this actor to the vulnerable object, and the function that maps the set of tools $\{T_i(t)\}$ to the value of the qualitative scale: $T \to S$, were T is a set of possible tools, S is a qualitative scale: $S =$ {critically dangerous, dangerous, slightly dangerous, non-dangerous}.

Each object O_j has a specific value V_j and a specific location L_j. Let us suppose that the value of the object can change and the location is static: $O_j = \{V_j(t), L_j\}$.

So, the model of HA can be represented as a tuple: $HA_{ij} = \{A_i, O_j, p_{ij}, G_{ij}, t\}$, where p_{ij} is a probability of a hybrid attack HA_{ij} that the actor A_i will make against the object O_j at a time t, G_{ij} is a goal of the attack (Fig. 1).

Hybrid operation HO consists of a set of hybrid attacks $HO = [HA_1, ..., HA_n]$.

Hybrid operation HO has a strategic goal G that can be achieved by reaching a sequence of lower-level goals $[G_1, ..., G_n]$ corresponding to hybrid attacks $[HA_1, ..., HA_n]$.

VULNERABILITY MODEL

Under the influence of HA, the value of the object decreases. Let us suppose that a HA and a change in the object's value as a result of it occur at the same moment in time, and ΔV_{ij} is a change of the value of O_j under the influence of HA_{ij}. Fig. 2 shows a graph of the change in the value of the object O_i over time under the influence of HAs.

A change in the value of the object under the influence of hybrid attacks, which are carried out by an actor being in different states, can be represented

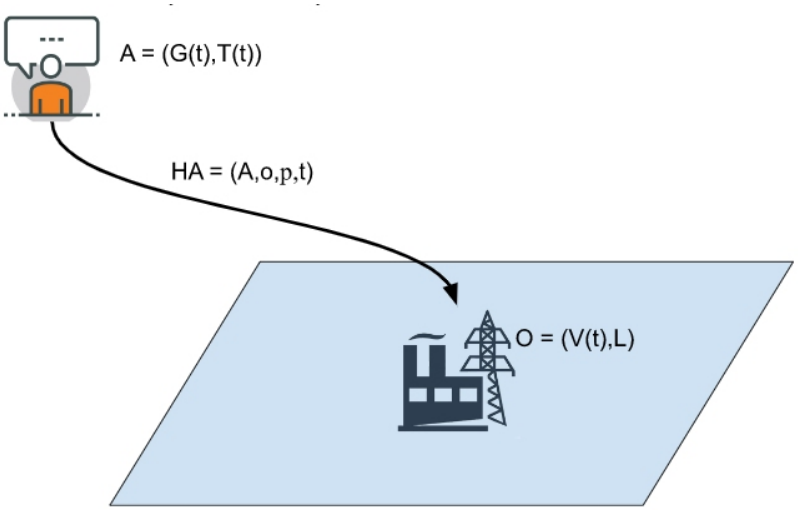

Figure 1: Hybrid attack model.

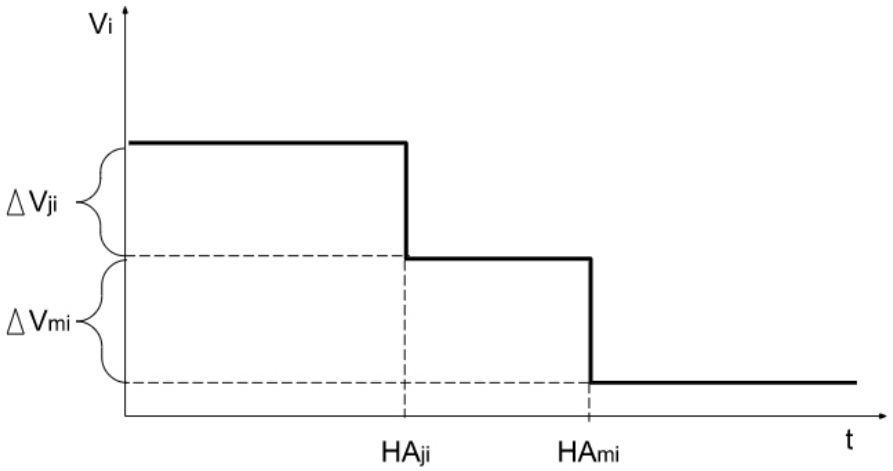

Figure 2: Graph of the change in the object's value.

Table 1. Table of the change in the object's value.

	O_1	O_2	...	O_n
S_1	ΔV_{11}	ΔV_{12}	...	ΔV_{1n}
S_2	ΔV_{21}	ΔV_{22}	...	ΔV_{2n}
...	...	...	...	...
S_m	ΔV_{m1}	ΔV_{m2}	...	ΔV_{mn}

in the form of table 1. The rows of table 1 correspond to the possible states of the actor, and the columns correspond to the vulnerable objects.

Table 1 represents the object vulnerability model and can be built for each potential actor.

Table 2. Table of potential risk from an actor being in different states for the objects.

	O_1	O_2	...	O_n
S_1, p_1	$R_{11}\left(p_{11}\left(HA/S_1\right), \Delta V_{11}\right)$	$R_{12}\left(p_{12}\left(HA/S_1\right), \Delta V_{12}\right)$	...	$R_{1n}\left(p_{1n}\left(HA/S_1\right), \Delta V_{1n}\right)$
S_2, p_2	$R_{21}\left(p_{21}\left(HA/S_2\right), \Delta V_{21}\right)$	$R_{22}\left(p_{22}\left(HA/S_2\right), \Delta V_{22}\right)$	...	$R_{2n}\left(p_{2n}\left(HA/S_2\right), \Delta V_{2n}\right)$
...	...	...	...	...
S_m, p_m	$R_{m1}\left(p_{m1}\left(HA/S_m\right), \Delta V_{m1}\right)$	$R_{m2}\left(p_{m2}\left(HA/S_m\right), \Delta V_{m2}\right)$	...	$R_{mn}\left(p_{mn}\left(HA/S_m\right), \Delta V_{mn}\right)$

HYBRID RISK ANALYSIS METHOD

Hybrid attack HA_{ij} is carried out by a certain actor A_i and is directed at a certain object O_j. For each actor, we can build a table that describes its possible states and the consequences of the actor's hybrid attacks on different vulnerable objects (table 2). Table 2 is built based on table 1.

p_i in the table 2 is a probability that the actor is in the state S_i, $p_{ij}\left(HA/S_i\right)$ is a conditional probability that the actor will attack the object O_j, given that the actor is in state S_i.

At the intersection of the rows and columns of table 2, there are values of risk that the actor being in the corresponding state will carry out a hybrid attack on the corresponding object. The risk is defined for each object as the product of the conditional probability of a hybrid attack and the change in the value of the object as a result of this attack: $R_{ij} = p_{ij}\left(HA/S_i\right) \times \Delta V_{ij}$.

Since risk is defined for each vulnerable object O_j that has a spatial reference (location L_j), the risk for this object also has the same spatial reference as the object. As a result of the implementation of hybrid attacks, the state of the actor, as well as the value of the object, will change. Therefore, the risk is a spatially distributed dynamic characteristic tied to the object and shows the potential damage to the object from a hybrid attack carried out by a certain actor.

Moreover, we propose to distinguish potential risks related to potential hybrid operations that have not yet occurred, real-time active risks related to active hybrid operations that are already identified, and post-crisis risk, which is determined by the assessment of recovery needs (Fig. 3).

FRAMEWORK STRUCTURE

The framework covers three stages of decision-making such as prevention, response, and recovery. For each stage, the framework contains a set of special tools, which are divided into two groups: monitoring and predicting hybrid attacks, as well as risk analysis (Fig. 3). For each of the three stages of decision-making, there is an analysis of potential risk, active risk, and post-crisis risk, respectively.

Risk analysis is based on attack monitoring and prediction models that use a case base (CB) as a repository of past or simulated HA scenarios together with decisions made to counter them. Potential risk analysis is based on forecasting the potential HAs. Active risk is assessed based on the monitoring of

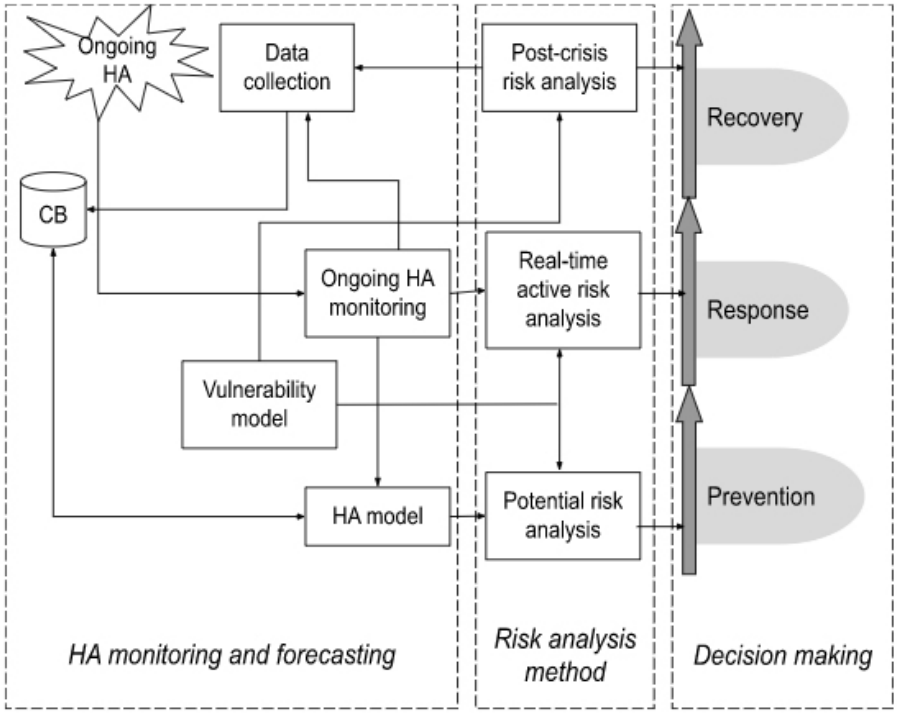

Figure 3: Framework structure.

ongoing attacks. The model of the vulnerability of vulnerable objects is used to analyze all types of risk.

CONCLUSION

The framework proposed in the paper offers a comprehensive approach to support decisions at all stages of the decision-making process. It brings together relevant tools to prevent, counter, and recover from the impact of HAs in a coordinated manner. The framework organizes specific tools in the groups corresponding to the stages of the decision-making process, each of which is based on risk assessment.

The division of risk into potential, active, and post-crisis risk allows making decisions corresponding to each of the three stages of the decision-making process. Spatially-distributed risk assessments allow us to highlight the most vulnerable areas that require priority attention.

During the attack prevention phase, these areas are formed based on a potential risk assessment, which considers existing vulnerabilities and is based on forecasting the potential HAs. Potential risk analysis aims at threat mitigation, identifying the most likely and impacting next steps for the attacker, enabling decision-makers to understand what can happen, which steps to take, and whether the community is truly prepared.

Decisions at the stage of countering the ongoing attacks are formed on the basis of the active risk assessment, for which active attacks are monitored.

Timely active risk analysis contributes to vigorous, coordinated responses to incidents limiting lost time, money, and the costs of recovery.

Decisions in the post-crisis stage are formed on the basis of post-crisis risk assessment. Post-crisis steps include assessments of the causes and of the management of the crisis and promulgation of lessons learned. In the post-crisis phase, it is also possible to correct the scenarios stored in the CB, as well as to develop new scenarios and replenish the CB.

REFERENCES

Bajarūnas E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View 2020, 19*(1), 62–70 © The Author(s) 2020 DOI: 10.1177/1781685820912041

Cyber Security Network of Competence Centres for Europe. (2019). *Periodic Reporting for period 2 - CyberSec4Europe (Cyber Security Network of Competence Centres for Europe)* DOI: 10.3030/830929

Diego, J.L., Martínez, I.L. (2022) EU-HYBNET: Empowering a Pan-European Network to Counter Hybrid Threats. *National Security and the Future*. 1(23) DOI:https://doi.org/10.37458/nstf.23.1.6

European Council. (2019). A new strategic agenda, 2019–2024. Brussels, 20 June. https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019–2024/. Accessed 14 February 2020

European Network for Cyber-security. (2019). *Periodic Reporting for period 2 - NeCS*. DOI 10.3030/675320 https://cordis.europa.eu/project/id/675320/reporting

European Union. (2022a) Protection of Critical Infrastructures from advanced combined cyber and physical threats https://cordis.europa.eu/project/id/101021274

European Union. (2022b) Disempowering Cyber-Attackers https://cordis.europa.eu/project/id/879953 DOI: 10.3030/879953

Giannopoulos, G., Smith, H., Theocharidou, M. (2021) The Landscape of Hybrid Threats: A conceptual model, *EUR 30585 EN, Publications Office of the European Unio*n, Luxembourg, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305

Hansen, P., Gill, M. (2021) Strategic Communications Hybrid Threats Toolkit Applying the principles of NATO Strategic Communications to understand and counter grey zone threats. ISBN: 978-9934-564-38-3

Zandee, D., van der Meer, S., Stoetman, A. (2021) Countering hybrid threats Steps for improving EU-NATO cooperation. *Clingendael Report* October 2021