a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

D5.3: Asset pricing and impact loss analysis: an empirical framework

Grant Agreement number:	833685
Project acronym:	SPIDER
Project title:	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
Start date of the project:	01/07/2019
Duration of the project:	36 months
Type of Action:	Innovation Action (IA)
Project Coordinator:	Name: Pier Luigi Polvanesi Phone: +39 010 600 2662 e-mail: pierluigi.polvanesi@ericsson.com

Due Date of Delivery:	07/01/2022
Actual Date of Delivery:	07/01/2022
Work Package:	WP5 – Economics of 5G Security
Type of the Deliverable:	Report
Dissemination level:	Public
Main Editors:	Michail Chronopoulos (CITY)
Version:	2.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

List of Authors, Contributors, Reviewers

Name	Role	Organisation
Maria Tsiodra	Author	CITY
Michail Chronopoulos	Co-Author	CITY
Matthias Ghering	Contributor	CLS
Irene Karapistoli	Contributor	CLS
Antonio Álvarez	Contributor	ATOS
Jorge Martinez Olmo	Contributor	ATOS
Panagiotis Gouvas	Contributor	UBITECH
Nikolaos Petroulakis	Reviewer	FORTH
Manos Athanatos	Reviewer	FORTH
Yiannis Tsampoulatidis	Reviewer	INF

History of Changes

Version	Date	Change History	Author	Organisation
0.1	12.04.2021	Initial version	Maria Tsiodra and Michail Chronopoulos	CITY
0.2	26.06.2021	Updated version. Contributions to Sections 2 and 3	Maria Tsiodra and Michail Chronopoulos	CITY
0.3	09.07.2021	Updated version. Contributions to Sections 2 and 3	Maria Tsiodra	CITY
0.4	12.07.2021	Updated version. Contributions to Sections 2, 3 and 8	Panagiotis Gouvas	UBITECH
0.5	26.07.2021	Updated version. Contributions to Sections 2 and 3	Matthias Ghering	CLS
0.6	30.07.2021	Updated version. Contributions to Sections 2 and 3	Jorge Martinez Olmo	ATOS
0.7	30.07.2021	Further work to submit document for internal review	Maria Tsiodra and Michail Chronopoulos	CITY
0.8	31.07.2021	Further work to submit document for internal review	Maria Tsiodra	CITY
0.9	01.08.2021	Cleaned-up version submitted for internal review	Maria Tsiodra	CITY
1.0	31.08.2021	Final version following internal review	Maria Tsiodra and Michail Chronopoulos	CITY
2.0	07.01.2022	Revised version following second review. The following changes are implemented: i. Clarification of the term *asset pricing* (a) Glossary, page 4. (b) Section 1, page 10. (c) Section 5, page 29. (d) Section 8, page 41. ii. Restructuring of Section 4.	Maria Tsiodra and Michail Chronopoulos	CITY

The content of this deliverable is PUBLIC and must be handled according to SPIDER Consortium Agreement.

Glossary

Term	Explanation
Asset Pricing	Evaluation of a 5G asset via the impact of a cyber attack using the DCF approach.
APT	Advanced Persistent Threat
CIC	Cybersecurity Investment Component
CRAE	Continuous Risk Assessment Engine
CVaR	Condition Valua at Risk
DCF	Discounted cash Flow
DMZ	Demilitarised Zone
GDPR	General Data Protection Regulation
PV	Present Value
NPV	Net Present Value
SME	Subject Matter Experts
VaR	Value at Risk

Disclaimer

The information, documentation and figures available in this deliverable are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability.

Contents

1 EXECUTIVE SUMMARY **10**

2 INTRODUCTION **11**

2.1 PURPOSE AND SCOPE . . . 11

2.2 MOTIVATION . . . 11

2.3 RELATION TO OTHER WORK IN THE PROJECT . . . 13

2.3.1 INTER CONNECTIONS . . . 13

2.3.2 INTRA CONNECTIONS . . . 14

2.4 STRUCTURE OF THE DOCUMENT . . . 17

3 METHODOLOGY FOLLOWED TO PRODUCE THIS DELIVERABLE **18**

3.1 DATA COLLECTION . . . 18

3.1.1 QUALITATIVE DATA . . . 18

3.1.2 QUANTITATIVE DATA . . . 19

3.2 EVALUATION FRAMEWORK . . . 21

3.3 DEMONSTRATION . . . 22

3.4 INNOVATION . . . 24

4 BASELINE KNOWLEDGE **25**

4.1 TRADITIONAL RISK ASSESSMENT MODELS . . . 25

4.2 EXTENSIONS OF TRADITIONAL LITERATURE . . . 27

5 WORK DEVELOPED **29**

6 CYBER RISK ASSESSMENT FRAMEWORK **31**

6.1 SYSTEM MODEL . . . 31

6.2 EXPECTED IMPACT . . . 32

6.3 PRESENT VALUE OF THE IMPACT . . . 34

7 ANALYSIS **36**

7.1 RISK ASSESSMENT . . . 36

7.1.1 FIRST PHASE . . . 36

7.1.2 SECOND PHASE . . . 37

7.1.3 n-th PHASE . . . 39

8 APPLICATION TO 5G NETWORKS **41**

9 CONCLUSIONS **46**

10 APPENDIX **47**

10.1 LIST OF ASSETS 47

10.2 LIST OF VULNERABILITIES 48

10.3 PHASE 1 49

10.4 PHASE n 50

List of Figures

1 WP5 reference architecture. . . . 13
2 Partial view of the SPIDER reference architecture. . . . 14
3 Overview of the CIC architecture. . . . 15
4 Overview of the DCF method. . . . 21
5 Diagrammatic overview of a network topology. . . . 22
6 Simulation of the financial impact of cyber attack. . . . 23
7 Possible security breach scenario. . . . 33
8 Sequential, multi-phase security breach. . . . 34
9 Attack graph representing the attacker actions in a vulnerable artificial 5G infrastructure. 41
10 High-level attack graph representing the attacker actions in a vulnerable artificial 5G infrastructure. . . . 42
11 Distribution of the PV of the impact for each asset of the network following a security breach. . . . 43
12 Indicative list of assets. . . . 47
13 Indicative list of vulnerabilities. . . . 48

List of Tables

1 List of symbols. 31
2 5G network sample characteristics 41
3 Parameter values and asset pricing. 42
4 Impact loss analysis. 45

1 EXECUTIVE SUMMARY

Assessing and controlling cyber risk is the cornerstone of information security management. However, these tasks are notoriously challenging not only due to the uncertainties associated with a cyber attack and the resulting risk exposure for an organisation, but also due to the availability of scarce resources for investment in mitigation measures. In this report, we develop an *asset pricing* and *impact loss analysis* (APILA) framework for gauging how a firm's financial risk exposure depends on key uncertainties underlying a cyber security breach. First, in the *asset pricing* part of the analysis, we evaluate the financial impact that a firm incurs as a result of a cyber security breach that progresses in phases. The latter is a critical aspect of the analysis as it not only signifies the serial approach to exploiting a system's vulnerabilities, but also facilitates the application of the discounting cash flow method for analysing how key uncertainties may affect the impact of a security breach. Second, in the *impact loss analysis* part of the framework, we assume that the duration of an attack phase, i.e. the time required to exploit a vulnerability, is a random variable and we derive a closed-form expression for the distribution of the Present Value (PV) of the financial impact of the cyber attack. In turn, this facilitates the development of key risk metrics that can be subsequently used to formulate optimisation objectives for deriving the optimal set of mitigation measures.

2 INTRODUCTION

2.1 PURPOSE AND SCOPE

The impact of a cyber attack can vary significantly depending on the type of security breach, the size of the organisation, industry and country and how well prepared it was. The APILA framework aims to estimate the impact of a cyber attack against various assets of an organisation and derive risk metrics to assess the implications of key underlying uncertainties. Hence, this report will start by identifying the assets that an organisation typically needs to protect. The objective is to estimate the economic implications of a cyber attack, in order to facilitate the evaluation of the economic sustainability of different controls. Specifically, we develop a method for classifying vulnerabilities based on the financial risk exposure they may entail if compromised, while loss analysis is carried out by measuring the system's risk exposure under a given configuration using standard risk measures, such as Value at Risk (VaR) and Conditional VaR (CVaR). Subsequently, these risk measures will be utilised in the optimisation models of D5.4 [3] in order to facilitate informed investment decisions in relation to measures for mitigating vulnerabilities, taking into account possible interdependences between them and various constraints.

2.2 MOTIVATION

Cyber defence is a standard part of enterprises' agenda, whereas hackers improve upon their techniques, thereby increasing the cyber risk levels around the world. Hence, assessing cyber risk is not just a necessary process that enterprises must conduct, but a natural way to realise the exact weaknesses, threats, and current security level of an organisation towards mitigating this risk. The existence of several tools that assess cyber risk and a vast number of papers and textbooks in this field demonstrates the importance of the risk assessment domain for both the industry and academia, as well as the wide variety of challenges to be addressed with this domain [12, 22, 30, 35]. Among the challenges that organisations must tackle in order to improve their cyber security posture, is that of gauging the financial impact of cyber breaches. This is a particularly critical task because it provides the necessary input for the formulation of models that address the optimal selection of mitigation measures.

Addressing these challenges is important, as, for example, the General Data Protection Regulation (GDPR) poses fines up to 20 million euros, or, in the case of an undertaking, up to 4% of the total turnover of the preceding financial year, whichever is higher [48]. However, these challenges are far from trivial, since overcoming them requires the development of novel techniques that combine risk

assessment and control optimisation in a way that accounts for critical aspects of the cyber attack itself, the relevant underlying uncertainties and constraints associated with the selection of mitigation measures [19, 45]. Examples of key uncertainties associated with a cyber attack is the *time required to exploit* a vulnerability before moving to the next one and the *extent of the associated impact* (cost) to the targeted organisation. Indeed, both exploitation time and cyber impact are likely to vary randomly, as they depend not only on the skills of the attacker but also on the level of cyber preparedness and response of the organisation.

Furthermore, an advanced cyber attack, like an Advanced Persistent Threat (APT), typically breaches its targets in *phases*, thus reflecting the process in which an adversary gradually exploits a series of system-, network- or even user-oriented vulnerabilities [52]. Advanced attacks may also remain stealthy inside a system seeking for available vulnerabilities to exploit. APTs are considered as a major threat attacking systems not only in multiple phases but for a highly variable period of time. The number of days an adversary remains in a targeted network before they are detected is referred to as *dwell time*. For example, the FireEye M-Trends 2020 Special report found that the mean dwell time for 2019 in the USA is 60 days and in both EMEA and APAC is 54 days [21]. This varying time spent by the attacker during each attack phase is associated with the risk inflicted by the presence of a threat actor within a system. Therefore, each phase poses its own risk value, which depends on both the exploitation time and characteristics of the available vulnerabilities.

In this report, we develop a framework for assessing the financial impact of a cyber attack by accounting for the serial nature of a cyber security breach and the uncertainty in the time required to exploit a vulnerability. Consequently, the contribution of this framework is two-fold: First, we incorporate key uncertainties into the traditional Discounted Cash Flow (DCF) method in order to make it more suitable not only for cyber risk assessment and investment decision-making, but also for supporting risk management within a 5G cyber security context. Second, we develop a case study, as in [20], for the purpose of demonstrating the application potential of this framework in a highly innovative area of telecommunications. To the best of our knowledge, this framework is the first that adopts a DCF approach to modelling and assessing cyber risk for multi-phase attacks taking into account the uncertainty in the duration of each phase, and proposes risk metrics as inputs to optimisation objectives that address the optimal selection of mitigation measures. Such a framework can assist decision makers and system administrators to allocate limited resources to patch vulnerabilities and contain advanced threats such as APTs.

2.3 RELATION TO OTHER WORK IN THE PROJECT

A diagrammatic overview of the connection of the different tasks within WP5 as well as between WP5 and the general SPIDER platform is indicated in Figure 1. Note that, as this report relates to D5.3, the relevant task is circled in red. Specifically, Figure 1 indicates: **i.** how the SPIDER simulated/emulated infrastructure as well as the SPIDER platform infrastructure provide data to be utilised within WP5; **ii.** the nature of the information and the way that this information is passed from one WP5 module to another; and **iii.** how the output of WP5 is reported to different SPIDER visualisation components.

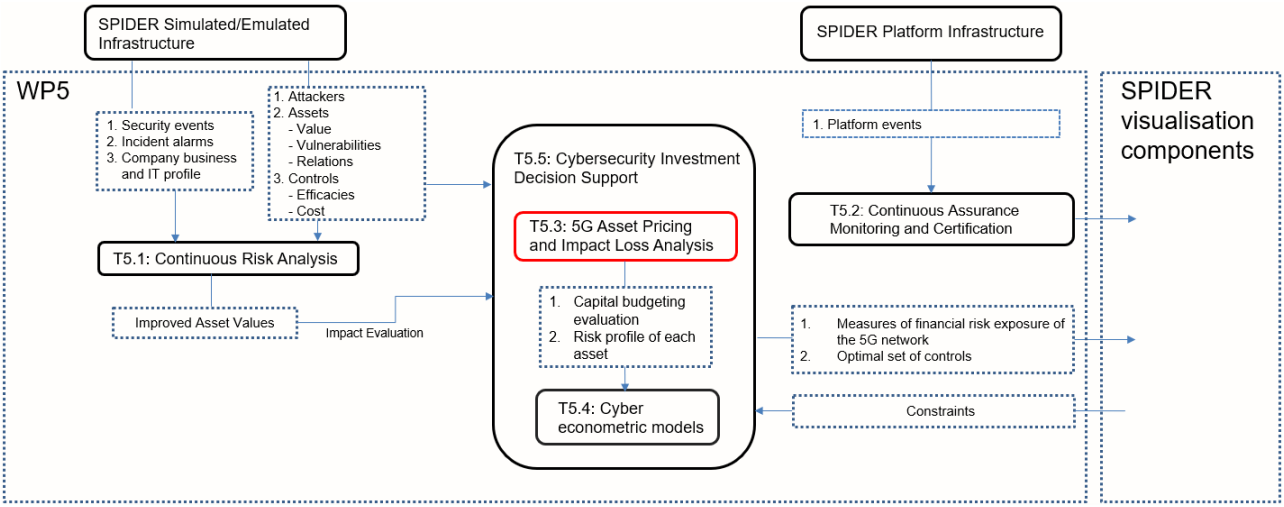

Figure 1: WP5 reference architecture.

2.3.1 INTER CONNECTIONS

There are two main links between WP5 and the general SPIDER platform. The latter is identified in Figure 1 and is decomposed as described below:

i The SPIDER Simulated/Emulated Infrastructure

Through the SPIDER Simulated/Emulated Infrastructure information is collected about security events, incident alarms as well as the company, business and IT profile. This information is passed on to T5.1 to be analysed by the Continuous Risk Assessment Engine (CRAE). Additionally, information about Attackers, Assets and Controls are also collected by the SPIDER Simulated/Emulated Infrastructure and passed on to T5.1 as well as T5.5.

ii The SPIDER Platform Infrastructure

The SPIDER Platform Infrastructure collects information about platform events and passes them on to T5.2. Hence, T5.2 is not directly linked with the quantitative analysis of WP5, but is part of it in terms of: **i.** developing the necessary mechanisms (a.k.a. controls) to ensure the security and privacy of the data held in the SPIDER platform, i.e. the protection of the platform itself; and **ii.** providing a real-time view of the security posture of the protected organisation where SPIDER is deployed.

2.3.2 INTRA CONNECTIONS

In order to demonstrate the strategic positioning of the APILA framework, we discuss here how T5.3 communicates with other elements within WP5. Note that the quantitative analysis within WP5 begins with T5.1 [2], which is designed to provide risk model templates to enable cyber risk analysis of target systems. Specifically, T5.1 receives data from the SPIDER Simulated/Emulated Infrastructure and provides *improved* information on asset values to T5.5, i.e. the Cybersecurity Investment Component (CIC). As indicated in Figure 1, in addition to this input, the CIC also receives information on attackers, assets and controls directly from the SPIDER Simulated/Emulated Infrastructure, and, together with the information from T5.1, the CIC calls the methodologies developed in the APILA framework.

More specifically, the CIC is highlighted in red in the partial view of the SPIDER reference architecture (developed in D2.7 [1]) presented in Figure 2. As shown in the SPIDER platform's reference architecture, the CIC receives the improved asset values from the CRAE, i.e. the part of SPIDER that calculates risks and asset value based on given assets relationships, vulnerabilities, controls, and threat appetites.

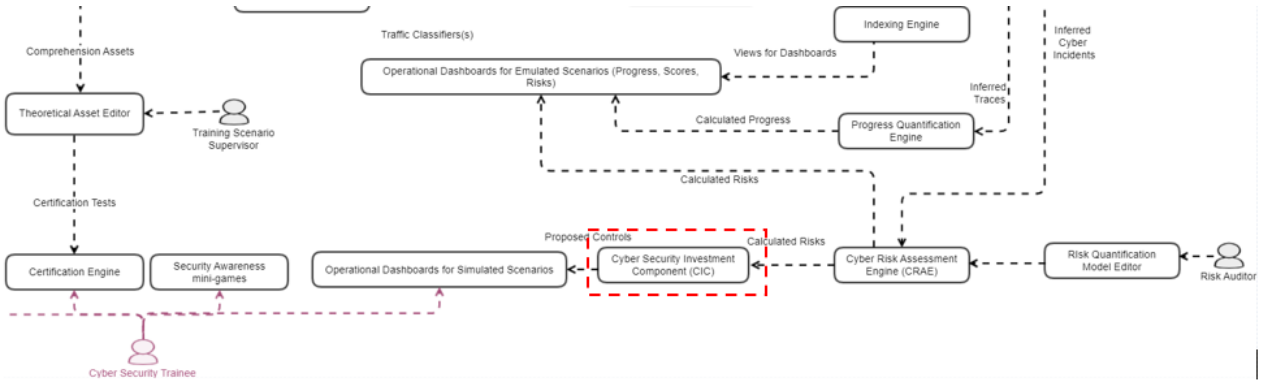

Figure 2: Partial view of the SPIDER reference architecture.

Although the final details about the CIC will be given in D5.7 [4], below, we describe briefly the main elements of the CIC, among which D5.3 plays a vital role, and illustrate them in Figure 3 in order to

demonstrate the position of the D5.3 relative to the other WP5 elements. Note that although Figures 1 and 3 illustrate similar information, there is a discrepancy in terms of exposition as they reflect different levels of abstraction.

i. The CRAE receives the same scenario data from the SPIDER platform as the CIC. Using this data it computes an improved asset value and provides this to the CIC.

ii. The SPIDER Dashboard, feeds the CIC with a variety of user data, including budget constraints, preferred optimisation strategies and additional control-related user preferences.

iii. The Kafka stream helps the CIC to interact with other SPIDER components including the SPIDER platform, the CRAE and the SPIDER Dashboard. It parses the data coming from the CRAE as well as the input coming from the SPIDER Dashboard and stores it within the User/System database (DB).

iv. The User/System DB stores the data collected by the Kafka stream and aggregates it for later use by the Economic Models. Some of this data can be fed back to the Kafka stream in the form of statistics, such that they can be visualised by the SPIDER Dashboard. Since the SPIDER Dashboard, SPIDER Platform, and CRAE can all continuously update, it is important that the CIC must first wait until it has obtained an adequate amount of information in order to calculate an optimal decision, and will have to automatically recalculate its decision when new data arrives.

v. The Economic Models use the data stored in the CIC's database to evaluate the impact of a serial cyber security breach.

vi. The valuation produced by the Economic Models will be optimised by the Control Optimisation. This process results in a set of optimal controls given constraints provided by the user.

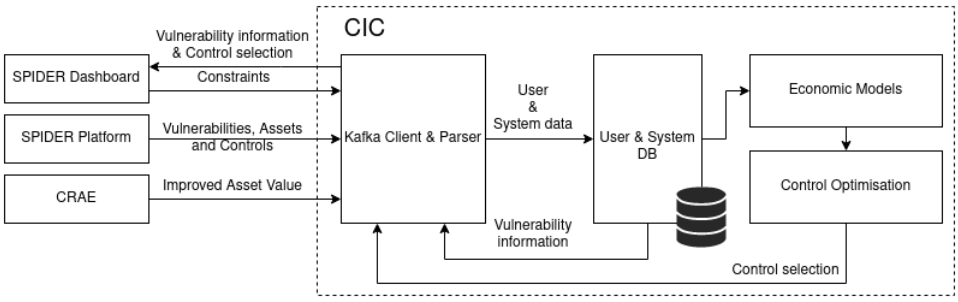

Figure 3: Overview of the CIC architecture.

Note that the APILA framework developed in D5.3 builds upon and complements the risk assessment framework of the CRAE. Indeed, the former receives input from the CRAE on key 5G network elements (e.g. assets), which, in turn, enables the integration of D5.3 within the general SPIDER platform and facilitates a coherent risk assessment framework. In addition, D5.3 utilises and extends traditional capital budgeting techniques in a way that facilitates an advanced evaluation of the impact of a cyber attack by incorporating key underlying uncertainties. Hence, viewed as an independent tool, the contribution of D5.3 is that it proposes an advancement of traditional evaluation and risk assessment techniques. However, viewed as part of the CIC, D5.3 facilitates the development of risk measures that will be passed on to D5.4 [3]. In turn, the latter aims to develop a decision support framework underlying the SPIDER's CIC via an optimisation model for addressing the problem of optimal allocation of a limited budget to a subset of available controls. Finally, the output from both D5.3 and D5.4 is returned to the CIC to be reported to different SPIDER visualisation components.

2.4 STRUCTURE OF THE DOCUMENT

The report is organised as follows. In Section 3, we present an overview of the methodology that consists of three main components: **i.** data collection; **ii.** evaluation framework; and **iii.** demonstration. Specifically, the process of data collection is presented in Section 3.1, which describes the nature of the data and how it is passed on from one SPIDER component to another. Also, Section 3.2 presents an overview of how the DCF method is utilised not only for the purpose of asset evaluation but also for risk assessment. Furthermore, Section 3.3 provides a high-level demonstration of the output of the APILA framework, while Section 3.4 concludes with an overview of the novelty and innovation of this work relevant to the existing literature.

Subsequently, we proceed by discussing in Section 4 the relevant literature in order to emphasise how the proposed framework contributes to existing risk assessment frameworks within the area cyber security economics. Specifically, the literature review demonstrates how the APILA framework builds upon and extends the traditionally static DCF method by incorporating key uncertainties. Thus, we emphasise how we improve this method by making it more appropriate for not only asset evaluation but also risk assessment within a cyber security context. Further discussion on the work developed in this report is presented in Section 5.

Next, in Section 6, we proceed with the quantitative part of the analysis that begins with the presentation of the assumptions and the notation that will be used throughout the report. We begin the analysis by deriving the expected PV for the first phase of an n-phase attack in Section 7.1.1. Subsequently, in Sections 7.1.2 and 7.1.3, we derive the analytical expression of the expected PV for phase 2 and phase n, respectively. Section 8 presents the application potential of the APILA framework via a simple toy example and Section 9 concludes the report.

3 METHODOLOGY FOLLOWED TO PRODUCE THIS DELIVERABLE

3.1 DATA COLLECTION

We begin the description of the methodology with an overview of the key input on which it is based. Specifically, we include below a preliminary description of key qualitative network elements, such as, the assets and their associated vulnerabilities, as well as a description of quantitative data regarding asset values, probability of attack and probability of successful exploitation per vulnerability of each asset.

3.1.1 QUALITATIVE DATA

- **Assets (**$i = 1, 2, \ldots, n$**)**

  An asset is defined as an item of value to achievement of organisational mission/business objectives [42]. Assets can either be tangible objects (e.g. hardware, software, computing platform, network device, or other technology components), or intangible (e.g. information, data, trademark, copyright, patent, intellectual property, or reputation). The aim of cyber security is to safeguard the confidentiality, integrity and availability of the organisation's assets. An indicative list of assets is included in Figure 12.

- **Vulnerabilities (**$j = 1, 2, \ldots, m_i$**)**

  A vulnerability is defined as a weakness in an information system, system security procedures, internal controls, or implementation that can be exploited or triggered by a threat [42]. Vulnerabilities can be leveraged by adversaries to gain access to an asset, change the asset's state or move laterally to another asset.

  The SPIDER platform provides a full list of vulnerabilities present in the system's environment. Each vulnerability is associated with a unique identifier, attack vector, attack complexity, required authentication and likelihood of being attacked.

  In addition to a list of assets and a list of vulnerabilities, the data provided by the SPIDER components also contains the relations between assets and vulnerabilities. These relations can be used to construct an attack graph, with the assets (or asset states) denoted as nodes, and the vulnerabilities represented as the transitions between these nodes.

  Information regarding the assets, vulnerabilities and their relations (attack paths) in an organisation environment can be manually obtained from Subject Matter Experts (SMEs) or using au-

tomated processes [51]. In our models we make use of data provided by other SPIDER components. This data includes a list of tangible assets in the environment with their associated value and identifiers. Intangible assets are indirectly included into the value of the tangible assets (e.g., valuable data increases the value of the database in which it is contained, or the server hosting the database). An indicative list of vulnerabilities is indicated in Figure 13.

3.1.2 QUANTITATIVE DATA

A description of quantitative data in relation to the aforementioned indicative list of assets and vulnerabilities are included below.

- **(Improved) Asset values**, A_i

  Asset valuation is one of the core steps of the risk assessment process and needs to consider the context and particularities of the organization being evaluated, the asset particularities, and the scenario characteristics. However, first and foremost, it should be clarified that there is no specific norm or rule of thumb to define the objective value of an asset within a network.

  Many methodologies can be followed or even combined together. The most prominent one is to bind the value of an asset with the CIA (Confidentiality, Integrity and Availability) consequences of a potential exploitation. The weights that affect the asset score depend on the nature of the asset, i.e. someone could start by a de-normalized value of [0.33C+0.33I+0.34A], then adjust the coefficients based on the asset nature, and, finally, apply a multiplication factor that would project the intermediate calculation to the axis of cost.

  Although this impact-based formula is very pragmatic, since it takes under consideration the operational aspect of the nodes, it overlooks one parameter that is highly crucial; which is "the usage of a node as a hacking stepping stone". Most of the time, adversaries try to spot the achilles heel of an infrastructure that will simplify the overall exploitation. Such assets include domain controller, ldap registries, credential repositories, etc. In the frame of SPIDER these parameters are taken under consideration.

  In terms of T5.1, based on an initial Asset Value quantitative metric provided by the Spider platform, the CRAE determines the improved asset values that will be used by the models at CRAE (D5.1) and CIC (D5.3). Specifically, the CRAE considers the company profile information in the risk assessment process. This information can include the information sent by the SPIDER platform, and the business profile that can be edited through a personalized questionnaire at the CRAE

interface. This questionnaire allows for a high level of personalization for each of the scenarios.

Furthermore, the CIA characteristics of an asset are also considered to determine the asset value. At CRAE, they range from 0 to 10, and can be edited using an asset questionnaire where it is also possible to indicate if the data used can be considered as "personal data" that may also influence the asset value, depending on the asset type and the scenario characteristics.

- **Probability of attack**, S_i, **and successful exploitation**, R_i

  Generally, there are two distinct ways to provide probabilities of attack and successful exploitation. The first one is the "ground-truth-oriented" while the second one is the "user-defined" or more precisely the "appetite-oriented" one. The "ground-truth-oriented" implies that there are specialized probes installed in various assets of the nodes (that constitute the service graph) and a fully-operational Security Operation Center (SOC) is able to interpret the raw-logs to processed Alerts. The produced data-stream of the alerts can be deterministically mapped to probability values. On the contrary, the appetite-oriented way makes use of global intelligence formulated by honeypots, security intelligence networks and disclosed statistics. The term 'appetite' derives from ISO27001, where risk officers are urged to perform risk calculations based on artificial probabilities. In this sense, a pessimistic appetite would imply that all attacks irrelevant of their complexity are highly probable or vice versa for an optimistic appetite. Finally, regarding the exploitability, it may be directly derived by the CVE metamodel. More specifically, the NIST calculations presented in https://www.first.org/cvss/specification-document may be fully inherited.

- **Exploitation hardness**

  The time to compromise or exploit a vulnerability is defined as the time required by an attacker to gain some level of privilege on some system component. This depends on a number of elements, such as the nature of the vulnerabilities and the attacker skill level. Consequently, the *exploitation hardness* is modelled as a random variable. Note that the APILA framework does not pose any restrictions on the type of distribution that exploitation hardness follows, however, for ease of exposition and demonstration, we will assume that exploitation hardness is an exponentially distributed random variable. Note that this assumption has been adopted in the existing literature [10], however, it has not been integrated within models for both risk assessment and optimisation of mitigation measures.

3.2 EVALUATION FRAMEWORK

The economic evaluation framework reflected in the asset pricing part of D5.3 builds upon the traditional DCF method. In finance, DCF analysis is a method of valuing a security, project, company, or asset using the concept of the time value of money. Specifically, DCF analysis determines the PV of a steam of cash flows based on estimations about its future evolution. In D5.3, we assume that a cyber attack is carried out in stages, which implies that its impact is realised at discrete points in time, and we adopt the DCF approach in order to estimate the PV of the overall impact of a cyber attack. This is illustrated in Figure 4 for the case where a cyber attack is carried out in three stages. Note that in order to compromise the first asset, the attacker requires an amount of time equal to T_1, and, similarly, the required amount of time for assets 2 and 3 is T_2 and T_3, respectively. Assuming a continuously compounded discount rate, denoted by ρ, the PV of the impact K_1 is $e^{-\rho T_1} K_1$. Thus, the PV is used to introduce the concept of discounting into the calculation of the current value of the impact of an attack that may require a substantial amount of time to be carried out. In turn, this supports effective decision-making [14] and facilitates the development of risk measures to assess the financial risk exposure of the defender.

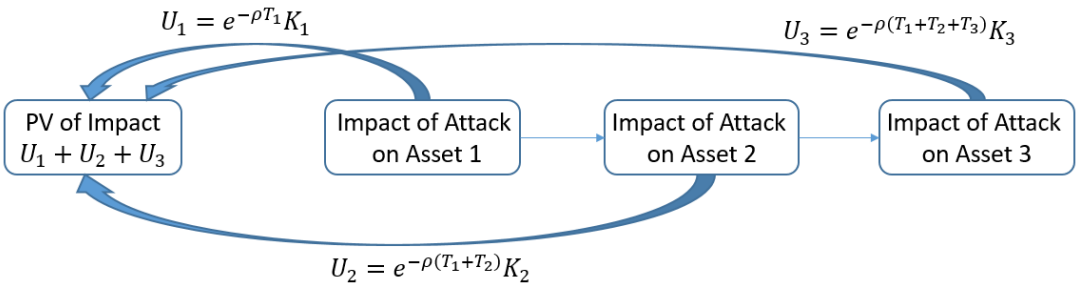

Figure 4: Overview of the DCF method.

Hence, the objective is to model the financial impact of a cyber attack by adopting a techno-economic approach that couples capital budgeting for evaluation of a serial cyber security breach with key underlying uncertainties. In terms of context, the evaluation framework consists of the underlying system model with an organisation that wishes to protect its systems and hackers who target the organisation, and a network of different system assets that inherently host interconnected vulnerabilities, and, as a result, can be sequentially compromised via a multi-phase attack.

3.3 DEMONSTRATION

Although the demonstration of the APILA framework will be presented thoroughly in D7.4 [5], here we provide a preliminary overview of the context within which the case study (in the form of a toy example) demonstrating the application potential of the APILA framework will be developed. Note that the APILA framework is flexible to support risk assessment in a wide range of contexts, however, it requires two key elements. First, it assumes that the cyber attack is carried out in discrete stages [51]. Second, in each stage the attacker exploits an asset of the network by compromising any one of its vulnerabilities. Therefore, for illustration purposes, we may consider a high-level context where a sample network topology depicts the inter-connectivity between different assets in each layer of a network architecture. For example, we may assume that the latter consists of three layers, namely the demilitarised zone (DMZ), the Intranet (or Middleware) and the Private Network, as illustrated in Figure 5. Each layer of the architecture may signify the importance of the asset to the organisation and the level of security the attacker has to breach or bypass to successfully exploit a vulnerability, and, in turn, an asset, thereby moving to the next layer.

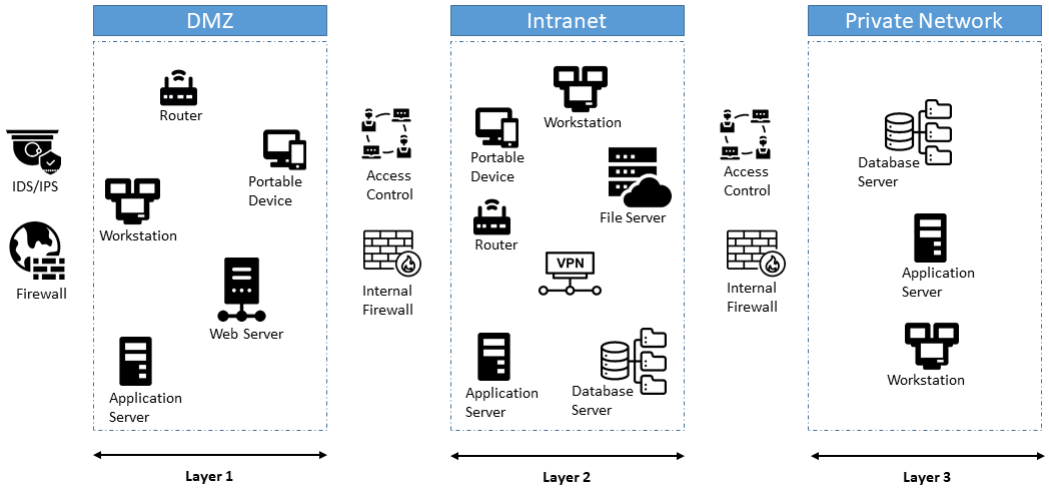

Figure 5: Diagrammatic overview of a network topology.

Once the relevant network (quantitative and qualitative) characteristics are collected, we proceed with the evaluation of the impact of a cyber attack for each asset taking into account the implications of exploitation hardness as well as the probabilities of attack and successful exploitation per vulnerability. Thus, we are able to determine not only the impact level of a cyber attack but also its PV. Finally, since the time by which the impact level is discounted is random, the PV of the impact level is also a random

variable, which allows us to determine its distribution, and, in turn, key risk metrics. Indeed, by deriving the distribution of the PV of the impact level, we can obtain metrics for gauging the amount of risk exposure and utilise these to develop objectives for optimising the selection of mitigation measures.

Additionally, as indicated in Figure 6, we do not restrict the APILA framework with assumptions about the distribution of exploitation hardness, so that it can facilitate the analysis of a wide range of empirical data. Indeed, exploitation hardness may be different among the different assets, and, failing to account for this may result in cycles of over- or under-investment, and, in turn, capital intensive corrective policy actions. In the literature, a wide range of distributions have been adopted to reflect the randomness of activity duration. Examples of probability distributions that can represent the statistical properties of the random activity duration include the beta [7, 29], log-normal [33, 47] and phase-type distributions [13].

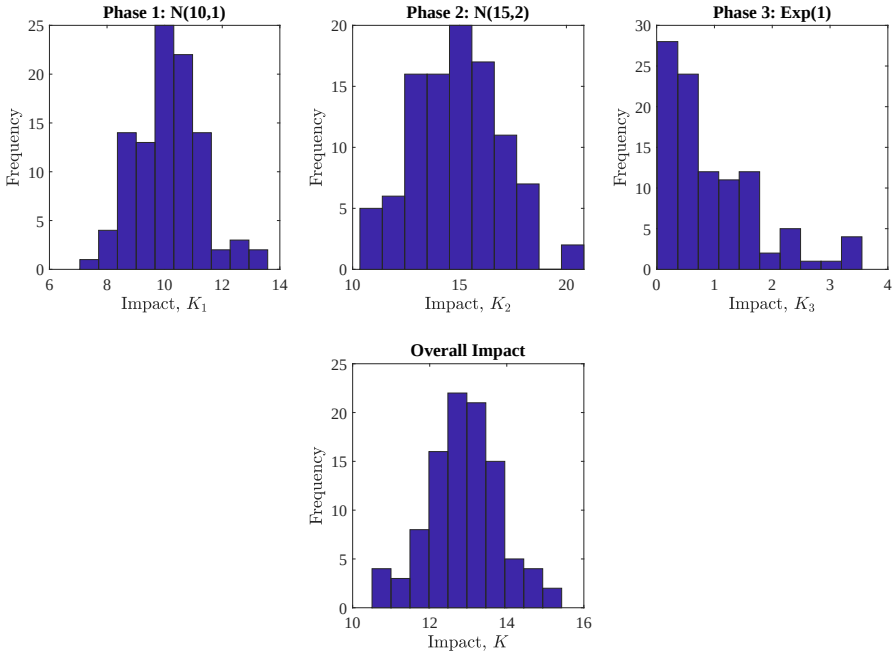

Figure 6: Simulation of the financial impact of cyber attack.

3.4 INNOVATION

The novelty of the APILA framework developed in D5.3 is reflected in the integration of key uncertainties within the DCF method and the flexibility of the latter to be adopted within optimisation methods for optimal selection of mitigation measures.

i. Capital budgeting techniques such as the DCF method have been utilised for project evaluation extensively. However, applications of this method typically ignore the implications of various underlying uncertainties. To address this disconnect, we develop a framework for evaluating the financial impact of a cyber attack that can facilitate critical uncertainties, and, thus, enable improved risk assessment.

ii. The time to exploit a vulnerability is recognised as an important aspect of a cyber attack. Indeed, it has been reported that it may take even months for an attack to be carried out successfully [32]. Despite its relevance and importance, this aspect has yet to be formally implemented within methods for evaluating the economic implications of cyber attacks.

iii. Among other things, the output of the APILA framework may include important risk metrics, e.g. VaR and CVaR, that can be used to gauge the financial risk exposure of a network following a cyber attack. Effectively, this enables a more formal treatment of cyber risk and opens up the potential to derive novel insights regarding financial aspects of cyber risk.

iv. The risk measures produced by the APILA framework can be integrated within the optimisation framework of D5.4 in order to drive the selection of mitigation measures. In turn, this facilitates the development of innovative software applications that offer decision support for risk management and investment in cyber security within the context of 5G networks.

4 BASELINE KNOWLEDGE

4.1 TRADITIONAL RISK ASSESSMENT MODELS

Risk management is a process of identifying risks and implementing plans to address them [8]. The essential parts of the risk management process are: **i.** risk assessment; and **ii.** risk control/mitigation. Thus, risk assessment is a sub-process of risk management consisting of risk identification and risk analysis. First, risk identification lists and classifies elements of risk, in terms of threats, vulnerabilities and impact. Then, risk is estimated with risk analysis. Generally, risk analysis requires two risk parameters, i.e. the probability of an attack and the amount of impact of the attack. This is typically formulated mathematically as:

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

Note that risk analysis can be quantitative or qualitative, depending on whether real values or abstract levels are used. The framework presented in D5.3 focuses on these two main tasks of risk assessment, and can, therefore, be decomposed as follows: First, an evaluator identifies the main parameters of risk. These may include valuable assets, possible threats and existing vulnerabilities in the security system. Second, risk is analysed by determining the likelihood and possible impact of an attack and aggregating these values.

As we will demonstrate in Sections 6, 7 and 8, the APILA framework will pave the way for the methodologies developed in D5.4 that address the second process of risk management, i.e. risk control. The latter is a sub-process for selecting and implementing measures to mitigate risks. Although there may be different alternative options, we will be mainly focusing on risk mitigation, which consists of actions helping to reduce risk (i.e. reduce the probability of a risky event occurrence, its impact or both). As it will be discussed more thoroughly in D5.4, a strand of the cyber security economics literature draws on the theory of investment and project valuation under uncertainty [11, 15], with the main objective to derive the expected value of investment in cyber security controls along with the investment threshold price and the probability of investment within a given time horizon [18]. As such, this work typically ignores the degree to which financial risk is hedged. In finance, the risk exposure of a project is measured by its VaR, which is the minimum project value for a given confidence level during a specified time horizon, and by its CVaR, which is the expected value of the project given that it is less than the VaR. Such risk measures are relevant in the area of cyber security and can be developed to gauge the financial risk exposure of an organisation following a security breach, however, applications within cyber security economics remain somewhat underdeveloped.

This is partly due to the difficulty of quantifying or estimating key parameters, such as the impact of a successful cyber attack. Indeed, quantifying the impact of a cyber attack is a fundamental factor for building risk assessment models [9, 17, 24]. However, the impact of a cyber attack may be very hard to quantify in advance because of the nature of information assets (e.g., private identifiable/health information), while reputation cost, which accounts for a large portion of the whole damage is very difficult to estimate. Not to mention that it is almost impossible to verify correctness of the estimated risks [27]. Additionally, the increasing number of interacting and evolving uncertainties underlying the attacks and the limited time to make executive decisions renders these models considerably complex.

Early examples of empirical models that focus on the development of risk measures, such the VaR and the CVaR, within a cyber security context include Wang *et al.* [49], who develop a model of investment in information security and utilise VaR to evaluate different investment tradeoffs. Specifically, using data on daily activities from a large US financial institution, they measure the risk of daily losses an organisation faces due to security exploits and use extreme value analysis to simulate the distribution of the daily losses and estimate the VaR. Thus, they develop a framework, whereby investment choice is based on a decision-maker's risk preferences instead of the minimization of the expected cost. Rakes *et al.* [39] present an integer programming model for determining optimal countermeasure selection based on threat likelihoods, under expected value and worst-case conditions. Their analysis is based on data on security threats, countermeasures and possible losses from successful breaches found in EndpointSecurity.org. An extension of this line of work is presented in Sawik [43], who utilises the same source of data but applies VaR and CVaR within the integer programming model of [39]. Also, taking the perspective of a smart grid, Law & Alpcan [31] investigate the impact of false data injection attacks, which threat the security of smart grid severely, by aiming at tampering meter measurements and affecting the results of state estimation. They present a game-theoretic approach to smart grid security by combining quantitative risk management techniques with decision making on protective measures. Results indicates that different risk measures may lead to different defence strategies, but the CVaR measure allows a decision maker to prioritise high-loss tail events.

More recently, Peng *et al.* [36] propose a novel application of marked point processes to fit and predict extreme cyber attack rates, while using the VaR to measure the intensity of cyber attacks. Using real-world data collected via network telescope and honeypot, they demonstrate how this approach offers accurate in-sample fitting and out-of-sample prediction performance. Also, Peng *et al.* [37] develop the first statistical approach based on a Copula-GARCH model that uses vine copulas to model the multivariate dependence of real-world cyber attack data. Results indicate that ignoring the multivariate dependence causes a severe underestimation of cyber security risks. Also, an investigation of the

optimal balance between prevention, detection and containment safeguards under uncertainty is presented in [28]. The authors find that adjusted prevention impacts social cost and optimal configuration of safeguards the most. They identify gaps in existing cyber security frameworks' reliance on prevention and propose recommendations addressing the gaps. In the direction of cyber security resilience, [16] develop a model based on the needed security controls to facilitate defined security functions. Considering affordable residual risk, budget, resiliency and usability constraints, the authors propose an optimal selection of critical security controls for optimal and resilient risk mitigation planning.

4.2 EXTENSIONS OF TRADITIONAL LITERATURE

Despite their contribution, the aforementioned models overlook key uncertainties, such as the time it takes to exploit a vulnerability and the cost that the system incurs once a vulnerability is compromised. However, such features must be implemented within quantification tools to assist in the anticipation and control of the financial impact of cyber attacks [23, 40]. For example, Arnold *et al*. [10] formalise the semantics of attack trees so as to allow their use for a probabilistic timed evaluation of attack scenarios. Specifically, they study the probability of a successful attack as time advances, to address the question: what is the probability that the system is successfully compromised within a given time interval? By utilising a framework based on acyclic phase-type distributions, they enable the derivation of the distribution of the time until the attack is successfully executed. Thus, their analysis of attacks is extending earlier time-abstract analyses [53] that considers only the probability of whether or not an attack eventually could take place, without evaluating the probability of success as a function of time.

In the same line of work, Harang and Kott [26] explore approaches to modelling the detection process of cyber infections on a computer network and analyse sets of intrusion detection records observed on networks of organizations protected by a form of intrusion detection and prevention service. Their results indicate that the timing of when the reports are filed is not uniformly distributed over a time interval but instead exhibits significant burstiness. Furthermore, they find that this burstiness can be modelled by a simple two-state model. In line with this result, we assume in this report that the time to exploit an asset of a network follows a generic probability distribution so that resulting risk assessment framework is flexible to be adopted for analysing a wide range of empirical data. In addition, unlike existing cyber risk-assessment models, we emphasise the serial nature of a cyber attack in order to establish a more accurate evaluation of its impact by integrating key uncertainties within traditional capital budgeting methods. Although the latter have been developed and adopted extensively for the evaluation of serial projects, their application potential has not be extended within

the context of cyber security.

Indeed, since our work focuses on assessing the risk associated with a security breach that progresses in phases, a more pertinent framework is that of Creemers [14], who studies the net present value (NPV) of a project with multiple phases that are executed in sequence. A cash flow may be incurred at the start of each phase and a payoff is obtained at the end of the project, while the duration of each phase is a random variable with a general distribution function. The novelty of this work is that it derives an exact closed-form expression for the moments of the NPV of a project as well as a closed-form approximation of the distribution of the project's NPV. By interpreting the randomness in the duration of each phase as the time required to exploit a vulnerability, we adopt and extend [14] within the context of cybersecurity, and derive risk measures to quantify the risk exposure that a security breach entails.

Specifically, the contribution of this work to the existing cyber security literature is threefold. First we develop a framework that integrates key uncertainties associated with a cyber attack within traditional capital budgeting methods, thereby rendering the latter more suitable not only for project evaluation but also risk assessment. Second, we evaluate not only the impact of a cyber attack but also its distribution, which, in turn, facilitates the development of measures for gauging the risk of a security breach. Third, we formulate objective functions using these risk measures that can be optimised to yield a set of mitigation measures.

5 WORK DEVELOPED

This report builds upon two main strands of the existing literature with the objective to extend the application potential of traditional evaluation and risk assessment frameworks within the area of cyber security economics and 5G networks. Consequently, the work developed in this report can be classified as follows:

i. Asset pricing

The process of *asset pricing* aims to determine the value of an asset as this is reflected upon the financial impact that a successful cyber attack would entail. In short, this process is twofold and consist of: **i.** incorporating the asset values obtained from D5.1 within the formula for evaluating the impact of a successful cyber attack on the assets of a 5G network; and **ii.** applying a discounting cash flow (DCF) method to determine the present value of the impact of a cyber attack for each asset of the network. This process takes into account the nature of the cyber attack and analyses the implications of key uncertainties associated with the impact of an attack and the time it takes to exploit an asset, which, in turn, facilitates a more rigorous treatment of risk.

Note that, although the alternative term of *asset valuation* may also be adopted, we have chosen *asset pricing* instead to avoid any overlap with the terms used in D5.1, which produces asset values to be utilised within D5.3, as demonstrated in Section 6.2 via Eq. (1).

ii. Impact loss analysis

Here we take a stylised approach to the modelling of key uncertainties associated with a cyber attack. Specifically, we assume that the time to exploit an asset is random as it may depend on the nature of the asset itself, the network's existing security infrastructure and the skills of the attacker. Allowing for such uncertainties within the DCF method, facilitates the process of risk assessment, as it enables the derivation of the distribution of the impact of a cyber attack and the associated risk metrics.

Note that the stepwise nature of a cyber attack implies that attacker exploits the assets of the network sequentially. Specifically, the attacker must exploit successfully one of the vulnerabilities of an asset of the network before moving on the next asset. In turn, this implies a connection between the assets through their vulnerabilities in a way that a successful attack formulates an attack path that goes through one vulnerability per asset, for all the assets of the network. Consequently, by changing the likelihood of an attack on a given vulnerability or the likelihood that

an attack is successful, we effectively alter the dependence among vulnerabilities and the propagation of an attack across a network.

6 CYBER RISK ASSESSMENT FRAMEWORK

In this section, we present our framework for modelling cyber risk by adopting a techno-economic approach that couples capital budgeting for valuation of a serial cyber security breach with key underlying uncertainties. In summary, this section discusses: **i.** the underlying system model with an organisation (defender) who wishes to protect its systems and hackers who target the organisation (attacker); **ii.** how the different system assets that inherently host vulnerabilities are linked to each other, and, as a result, how a *multi-phase attack* can sequentially compromise these assets causing damage to the defender; **iii.** how the DCF method can be adopted to gauge a system's financial risk exposure; and **iv.** how risk metrics can be developed into objectives for optimising the selection of mitigation measures. Note that part (iv) is directly relevant for the development of D5.4, where we will develop a set of techniques for optimising the selection of controls for mitigating the impact of a cyber attack under different constraints. Table 1 presents a summary of the notation used in this report.

Table 1: List of symbols.

Symbol	Description
i	phase of attack or an asset ($i = 1, 2, \ldots, n$)
$\mathcal{A}$	set of attack phases or assets
$\mathcal{V}$	set of vulnerabilities
v_{ij}	vulnerability within asset i ($j = 1, 2, \ldots, m_i$)
A_i	Value of asset i
R_{ij}	Probability of vulnerability v_{ij} being targeted (attack occurrence)
S_{ij}	Probability of vulnerability v_{ij} being compromised when attacked (success rate)
T_i	Time required to exploit asset i
W_k	Total duration of the attack until phase k, $\sum_{i=1}^{k} T_i$ where $1 \leq k \leq n$
K_i	Expected impact from exploiting asset i
U_i	PV of the expected impact for attack phase i
Z_n	Aggregated expected impact for the first n attack phases, $\sum_{i=1}^{k} U_i$ where $1 \leq k \leq n$

6.1 SYSTEM MODEL

We assume that the defender's infrastructure consists of a number of systems and networks, referred as assets, which the defender aims to protect from the attacker. The infrastructure can be represented as a directed acyclic graph of assets and vulnerabilities, where each asset $i \in \mathcal{A}$ has a set of vulnerabilities $\mathcal{V}_i = \{v_{i1}, v_{i2}, \ldots, v_{im_i}\}$ that the attacker may exploit. These vulnerabilities may be part of software weaknesses, as presented in the Common Weakness Enumeration (CWE)[1]. This assumption is aligned with the real world behaviour of attackers, who aim to compromise as many systems and penetrate as deep in the network as they can to increase their expected return from the attack.

[1] https://cwe.mitre.org/index.html

Subsequently, the value at risk for the defender increases with increase in the number of compromised systems. These adversarial interactions are modelled as a sequence of attack phases, where phase i of an attack refers to the stage in which the attacker aims to compromise asset i by exploiting any of its vulnerabilities $v_{ij} \in \mathcal{V}_i$. We assume that in each phase the attacker can compromise only one asset. A successful exploitation can lead to undesirable privilege escalation or lateral movement within the defender's infrastructure [34, 38], which presents a new set of vulnerabilities that the attacker can choose to exploit further and compromise the subsequent asset.

6.2 EXPECTED IMPACT

The impact from exploitation of asset i is denoted by K_i. Utilising the broadly accepted risk assessment formula [50], expected impact = (likelihood of being attacked) x (probability of being compromised) x (probable loss), we compute the impact as in (1).

$$K_i = A_i \cdot \langle R_i, S_i \rangle \tag{1}$$

This expresses the cyber risk posed to the defender during the i-th phase of an attack. In (1): A_i is the value of asset i (also known as Single Loss Expectancy (SLE) [46]); r_{ij} is the likelihood of the attacker attempting to exploit vulnerability v_{ij}, which expresses the degree of attractiveness of a vulnerability to the attacker, which the literature also refers to as the Annual Rate of Occurrence (ARO) [46]; and s_{ij} is the probability of the same vulnerability to be successfully breached. Further, s_{ij} captures the current *security level* associated with the vulnerability, which is analogous to the hardness in successfully exploiting the vulnerability. We express the likelihood of occurrence of an attack as, $\langle R_i, S_i \rangle$, which is the inner product between $R_i = (r_{i1}, r_{i2}, \ldots, r_{im_i})$ and $S_i = (s_{i1}, s_{i2}, \ldots, s_{im_i})$ of asset i [41].

As a high-level, illustrative example, consider an organisation with three assets. Let $\mathcal{V}_1 = \{v_{11}, v_{12}\}$, $\mathcal{V}_2 = \{v_{21}, v_{22}, v_{23}\}$, and $\mathcal{V}_3 = \{v_{31}, v_{32}\}$ be the set of vulnerabilities for assets $1, 2$ and 3, respectively. As there are three assets, the attack process involves three phases. In each phase, the attacker must compromise one asset to be able to realise and target vulnerabilities of the next asset. As the attack is a sequential process, the attacker would first need to exploit a vulnerability $v_{1j} \in \mathcal{V}_1$, which corresponds to the first asset before progressing to the next phase with vulnerabilities $\mathcal{V}_2$ that corresponds to the second asset, and, finally, to $\mathcal{V}_3$, i.e. the third asset. Figure 7 presents a network of associated vulnerabilities and the dashed red line highlights a possible attack path.

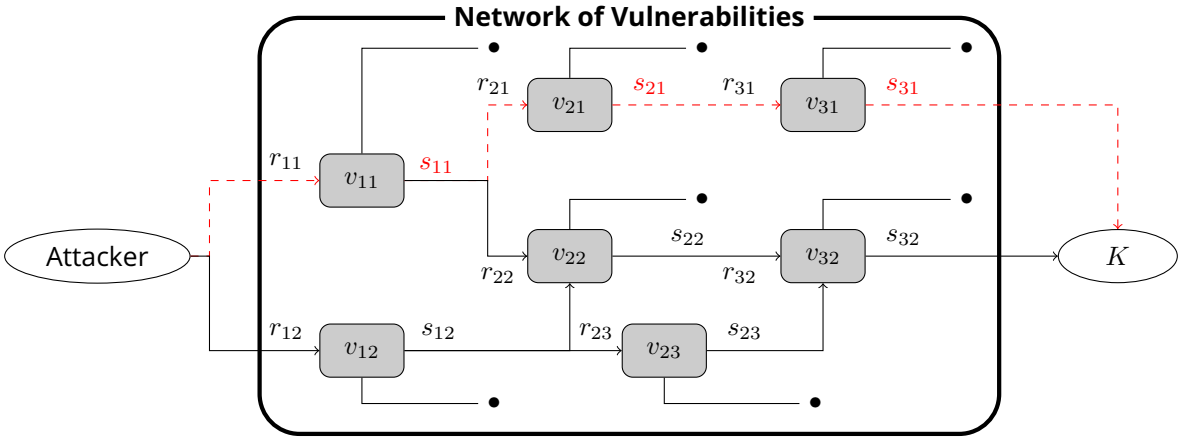

Figure 7: Possible security breach scenario.

For the purpose of demonstrating the functionality of the APILA framework within the context of D5.3, the relevant parameter values will be chosen randomly. Yet, based on empirical evidence, they will reflect aspects that are either endogenous, e.g. security level, or exogenous to the system, e.g. the skills of the attacker, which has not been model explicitly. Additionally, note that analysing aspects of propagation requires assumptions about the way that different probabilities are linked. Although we can chose the values of r_{ij} and s_{ij} to facilitate the analysis of any scenario of interest, we will not be considering a stylised relationship among them, nor will we be considering the conditional dependence among the different probabilities.

Furthermore, the calculation models developed for risk calculation and defensive strategy generation can be applied in any service graph that is arbitrarily defined. To this end, there are literally no restrictions on how these models are fed/initialized. As if the proper serialized input is valid and the graph is logically and syntactically correct, proper output can be produced and visualized. One of these graphs is the graph that has been proposed in the frame of the red-blue game that has been implemented. However, as already explained in the architecture deliverable, this graph is static and as such the potential of the calculation models would be radically decreased if algorithms were implemented 'within' the game. On the contrary, the strategic decision to create a general purpose editor that feeds the algorithms has been taken. Through this editor, any graph with any parameters can be used to trigger the elaborated calculations.

6.3 PRESENT VALUE OF THE IMPACT

For an attack phase i, T_i represents the time required to exploit a vulnerability v_{ij} in $\mathcal{V}_i$, and we refer to this as the hardness of exploiting a vulnerability. We assume that T_i follows a general distribution function denoted by $\Psi_{T_i}(\cdot)$, as shown in Figure 8. Assuming that a successful stealthy attack consists of a number of phases, each of them compromising an asset, we compute the duration of the attack (W_k) as the sum of the exploitation times required to compromise an asset in each phase, i.e. $W_k = \sum_{i=1}^{k} T_i, 1 \leq k \leq n$.

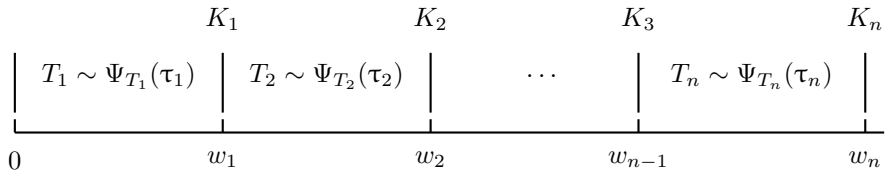

Figure 8: Sequential, multi-phase security breach.

To realise the expected impact that can materialise in the future, T5.3 determines the distribution of the PV of the expected impact associated with the attack. Equation (2) expresses the aggregated expected impact (Z_n) over n attack phases as

$$\begin{aligned} Z_n &= \underbrace{K_1 e^{-\rho W_1}}_{U_1} + \underbrace{K_2 e^{-\rho W_2}}_{U_2} + \cdots + \underbrace{K_n e^{-\rho W_n}}_{U_n} \\ &= \sum_{i=1}^{n} U_i \end{aligned} \tag{2}$$

where U_i is the PV of K_i, ρ denotes the discount rate and W_i the duration of the attack until phase i. The PV is used to introduce the concept of discounting into the calculation of the current value of variable, which supports effective decision-making [14]. In turn, this facilitates the development of risk measures to assess the financial risk exposure of the defender [25].

Indeed, the need to account for the discounting effect, which also reflects one of the novelties of the APILA framework, results from the potentially substantial time required to exploit a vulnerability. In various occasions this has been reported to extend to a period spanning several months. Additionally, the formulation in (2) emphasises another novelty of the APILA framework, as it demonstrates how uncertainty can be incorporated within a traditionally static capital budgeting method. By allowing for discounting, the randomness inherent in the time required to exploit a vulnerability is integrated within the formula for evaluating the PV of the impact of the cyber attack, which, in turn, renders the DCF method suitable not only as an evaluation but also as a risk assessment method.

After gauging the potential risk exposure associated with each vulnerability, D5.4 subsequently focuses on optimising the coverage of vulnerabilities in each asset by determining the appropriate Security Package. A security package refers to the implementation of cyber controls, which minimise the expected impact from an attack. This is done by patching asset vulnerabilities, thereby reducing its attack surface or by increasing the effort required in successfully breaching the asset. D5.4 specifically considers that the implementation of a control will mitigate the expected impact of an attack by reducing the probability of the latter being successful.

7 ANALYSIS

7.1 RISK ASSESSMENT

One of the main functionalities of the APILA framework is to assess the PV of the expected impact from a security breach. To achieve this, we perform a phase-wise analysis of a cyber attack to compute: **i.** The distribution of the PV of the expected impact at each phase $i = 1, 2, \ldots, n$; **ii.** The distribution of the PV of the aggregated expected impact (Z_n) over n phases; and **iii.** Risk measures to gauge the financial risk exposure following the multi-staged attack.

7.1.1 FIRST PHASE

We begin with the first of an n-phase attack, and assume that the phase starts at time 0 and stops at time $w_1 \equiv \tau_1$, which is a realisation of the random variable $W_1 \equiv T_1$. The PV of the expected impact, denoted by u_1, is described in (3), where ρ is the discount rate and τ_1 is the time at which the expected impact K_1 is realised.

$$u_1 = K_1 e^{-\rho\tau_1} \tag{3}$$

Consequently, the cumulative distribution function (cdf) and probability density function (pdf) of the PV of K_1 are given in (4) and (5), respectively (all proofs can be found in the Appendix). Note that (4) and (5) describe the general expression for the cdf and pdf of the PV, respectively, that assumes a generic distribution for T_1.

$$\Theta_{U_1}(u_1) = 1 - \Phi_1\left(\ln\left(\frac{K_1}{u_1}\right)\rho^{-1}\right) \tag{4}$$

$$\theta_{U_1}(u_1) = \frac{\phi_1\left(\ln\left(\frac{K_1}{u_1}\right)\rho^{-1}\right)}{ru_1} \tag{5}$$

If τ_1 is a realisation of the random variable T_1 that follows an exponential distribution with rate parameter λ_1, i.e. $T_1 \sim \exp(\lambda_1)$, then, for a given discount rate ρ, the cdf and pdf of the PV of K_1 is described in (6) and (7), respectively.

$$\Theta_{U_1}(u_1) = \left(\frac{u_1}{K_1}\right)^{\frac{\lambda_1}{\rho}} \tag{6}$$

$$\theta_{U_1}(u_1) = \frac{\lambda_1}{\rho}\left(\frac{u_1}{K_1}\right)^{\frac{\lambda_1}{\rho}-1}\frac{1}{K_1} \tag{7}$$

Next, having derived the analytical expression of the cdf and pdf of U_1, we can derive the main moments of the distribution. Thus, (8) and (9) indicate the expectation and variance, respectively.

$$\mathbb{E}[U_1] = \frac{\lambda_1}{\lambda_1+\rho}K_1 \tag{8}$$

$$\mathrm{Var}[U_1] = \left[\frac{\lambda_1}{\lambda_1+2\rho} - \left(\frac{\lambda_1}{\lambda_1+\rho}\right)^2\right]K_1^2 \tag{9}$$

The benefit from deriving the analytical expression for the distribution of U_1 is that we can now obtain the analytical expression for the VaR and the CVaR of the PV of the impact K_1. These risk measures can be used to gauge the financial risk exposure of the infrastructure from the first phase of the cyber attack, as shown in Proposition 1.

Proposition 1 *The* VaR *and* CVaR *of the expected impact of the phase 1 attack is:*

$$\mathrm{VaR}_\xi(U_1) = K_1(1-\xi)^{-\frac{\lambda_1}{\rho}} \tag{10}$$

$$\mathrm{CVaR}_\xi(U_1) = \frac{1}{\xi}\int_0^\xi \mathrm{VaR}_q(U_1)dq \tag{11}$$

7.1.2 SECOND PHASE

A cyber attack will most likely consist of more than one phases leading to the need for incrementally extending Section 7.1.1 to analyse two phases. Note that T_1 and T_2 do not necessarily follow the same distribution. Therefore, we start with the distribution of $W_2 = T_1 + T_2$ and assume that T_1 and T_2 follow exponential distributions with different parameters, i.e. $T_1 \sim \exp(\lambda_1)$ and $T_2 \sim \exp(\lambda_2)$. Consequently, W_2 follows a hypo-exponential distribution, i.e. $W_2 \sim \mathrm{Hypo}(\lambda_1, \lambda_2)$, with cdf and pdf described in (12) and (13), respectively [44].

$$\Phi_{W_2}(w_2) = 1 - \frac{\lambda_2}{\lambda_2-\lambda_1}e^{-\lambda_1 w_2} + \frac{\lambda_1}{\lambda_2-\lambda_1}e^{-\lambda_2 w_2} \tag{12}$$

$$\phi_{W_2}(w_2) = \frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}e^{-\lambda_2 w_2} - \frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}e^{-\lambda_1 w_2}. \tag{13}$$

Following the same steps as in section 7.1.1, we can determine the distribution of the PV of the impact associated with the second phase, as shown in Proposition 2.

Proposition 2 *If $W_2 \sim \text{Hypo}(\lambda_1, \lambda_2)$, then the cdf and pdf of u_2 is described in* (14) *and* (15)

$$\Theta_{U_2}(u_2) = \frac{\lambda_2}{\lambda_2 - \lambda_1}\left(\frac{u_2}{K_2}\right)^{\frac{\lambda_1}{\rho}} - \frac{\lambda_1}{\lambda_2 - \lambda_1}\left(\frac{u_2}{K_2}\right)^{\frac{\lambda_2}{\rho}} \tag{14}$$

$$\theta_{U_2}(u_2) = \frac{\lambda_1\lambda_2}{\lambda_2 - \lambda_1}\frac{1}{\rho u_2}\left[\left(\frac{u_2}{K_2}\right)^{\frac{\lambda_1}{\rho}} - \left(\frac{u_2}{K_2}\right)^{\frac{\lambda_2}{\rho}}\right] \tag{15}$$

while the mean and the variance of u_2 is described in (16) *and* (17)*, respectively.*

$$\mathbb{E}[U_2] = \frac{\lambda_1\lambda_2}{(\lambda_1 + \rho)(\lambda_2 + \rho)}K_2 \tag{16}$$

$$\text{Var}[U_2] = \frac{\lambda_1\lambda_2}{(\lambda_1 + 2\rho)(\lambda_2 + 2\rho)}K_2^2 - \frac{\lambda_1^2\lambda_2^2}{(\lambda_1 + \rho)^2(\lambda_2 + \rho)^2}K_2^2 \tag{17}$$

For completeness, we may also consider the special case where $\lambda_1 = \lambda_2 = \lambda$. This means that T_1 and T_2 are i.i.d. random variables, and, therefore, $W_2 \sim \text{Erlang}(2, \lambda)$ [44]. In this case, the cdf and pdf of W_2 are described in (18) and (19), respectively.

$$\widehat{\Phi}_{W_2}(w_2) = 1 - e^{-\lambda w_2}(1 + \lambda w_2) \tag{18}$$

$$\widehat{\phi}_{W_2}(w_2) = \int_{-\infty}^{+\infty} \widehat{\phi}_{T_1}(w_2 - \tau_2)\widehat{\phi}_{T_2}(\tau_2)d\tau_2 = \lambda^2 w_2 e^{-\lambda w_2} \tag{19}$$

Also, the cdf and pdf of the PV of the impact associated with the second phase is described in (20) and (21), respectively

$$\widehat{\Theta}_{U_2}(u_2) = \left(\frac{u_2}{K_2}\right)^{\frac{\lambda}{\rho}}\left[1 + \frac{\lambda}{r}\ln\left(\frac{K_2}{u_2}\right)\right] \tag{20}$$

$$\widehat{\theta}_{U_2}(u_2) = \left(\frac{\lambda}{\rho}\right)^2\left(\frac{u_2}{K_2}\right)^{\frac{\lambda}{\rho}-1}\frac{1}{K_2}\ln\left(\frac{K_2}{u_2}\right) \tag{21}$$

while the mean and the variance of U_2 is:

$$\mathbb{E}\left[U_2\right] = \left(\frac{\lambda}{\lambda + \rho}\right)^2 K_2 \tag{22}$$

$$\text{Var}\left[U_2\right] = \left[\left(\frac{\lambda}{\lambda + 2\rho}\right)^2 - \left(\frac{\lambda}{\lambda + \rho}\right)^4\right]K_2^2 \tag{23}$$

Following the same approach, we can derive the distribution of the PV of the impact for each phase, and, therefore, we proceed in Section 7.1.3 with the presentation of the general case. However, note that, although we can derive the analytical expression of the distribution of the expected impact for

phase i, the VaR and CVaR for $i > 1$ must be obtained numerically, since analytical expressions are not feasible.

7.1.3 n-th PHASE

The results of the previous sections (7.1.1 and 7.1.2) can now be generalised for the arbitrary n-th phase. In this case, $W_n \sim \text{Hypo}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and the cdf and pdf of W_n is described in (24) and (25), respectively [44].

$$\Phi_{W_n}(w_n) = 1 - \sum_{i=1}^{n} e^{-\lambda_i w_n} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \tag{24}$$

$$\phi_{W_n}(w_n) = \sum_{i=1}^{n} \lambda_i e^{-\lambda_1 w_n} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \tag{25}$$

Next, the cdf and pdf of U_n is obtained in a similar way as in the previous sections and is described in Proposition 3.

Proposition 3 *If $W_n \sim \text{Hypo}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, then the cdf and pdf of U_n is described in* (26) *and* (27)

$$\Theta_{U_n}(u_n) = \sum_{i=1}^{n} \left(\frac{u_n}{K_n}\right)^{\frac{\lambda_i}{\rho}} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \tag{26}$$

$$\theta_{U_n}(u_n) = \sum_{i=1}^{n} \frac{1}{rK_n} \left(\frac{u_n}{K_n}\right)^{\frac{\lambda_i}{\rho}} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \tag{27}$$

while the mean and variance of U_n is described in (28) *and* (29)*, respectively.*

$$\mathbb{E}[U_n] = K_n \sum_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \rho} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \tag{28}$$

$$\text{Var}[U_n] = K_n^2 \sum_{i=1}^{n} \frac{\lambda_i}{\lambda_i + 2\rho} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} - \left[K_n \sum_{i=1}^{n} \frac{\lambda_i}{\lambda_i + r} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i}\right]^2 \tag{29}$$

In the special case where $\lambda_i = \lambda, \forall i = 1, 2, \ldots, n$, the general expression for the cdf and pdf of U_n is described in (30) and (31), respectively.

$$\widehat{\Theta}_{U_n}(u_n) = e^{-\lambda w_n} \sum_{i=0}^{n} \frac{(\lambda w_n)^i}{i!}, \quad w_n = \frac{1}{\rho} \ln\left(\frac{K_n}{u_n}\right) \tag{30}$$

$$\widehat{\theta}_{U_n}(u_n) = \frac{1}{(n-1)!} \left(\frac{\lambda}{r}\right)^n \left(\frac{u_n}{K_n}\right)^{\frac{\lambda}{\rho}-1} \frac{1}{K_n} \ln\left(\frac{K_n}{u_n}\right)^{n-1} \tag{31}$$

The mean and variance of the arbitrary n-th phase is described in (32) and (33), respectively. Notice that an increase in n lowers the expected PV of the impact, which reflects the effect of discounting.

$$\mathbb{E}\left[U_n\right] = \left(\frac{\lambda}{\lambda+\rho}\right)^n K_n \tag{32}$$

$$\mathrm{Var}\left[U_n\right] = \left[\left(\frac{\lambda}{\lambda+2\rho}\right)^n - \left(\frac{\lambda}{\lambda+\rho}\right)^{2n}\right] K_n^2 \tag{33}$$

Having already derived the distribution of the PV of the impact for each phase, and, in turn, the mean of each PV, U_i, (refer to equations (8), (16), (28)), the expected PV of Z_n is given by (34).

$$\begin{aligned} Z_n = \sum_{i=1}^{n} U_i \Rightarrow \mathbb{E}[Z_n] &= \sum_{i=1}^{n} \mathbb{E}[U_i] \\ &= \sum_{g=1}^{n} K_g \sum_{i=1}^{g} \frac{\lambda_i}{\lambda_i + r} \prod_{j \neq i} \frac{\lambda_j}{\lambda_j - \lambda_i} \end{aligned} \tag{34}$$

Note that (34) can now be utilised within an optimisation framework to address the problem of optimal selection of mitigation measures. Specifically, the scope of the optimisation in this case would be to minimise the expected PV of the impact of a cyber attack subject to different constraints, e.g. budget constraint, which will be presented in D5.4.

8 APPLICATION TO 5G NETWORKS

We demonstrate the application potential of the APILA framework in a 5G case study motivated by the growing concerns over 5G security and major security events, such as the 2018-2019 soft cell campaign that affected more than 10 different telecommunication providers in 30 countries. As a motivating example, we consider a 5G network that consists of three assets. The vulnerabilities of each asset and the state of the attack once each vulnerability is compromised are indicated in Table 2. Notice that each asset has two vulnerabilities, i.e. $\dim \mathcal{V}_i = 2, \forall i \in \mathbb{N}$.

Table 2: 5G network sample characteristics

Asset 1	**State**	**Asset 2**	**State**	**Asset 3**	**State**
V_{11}: Brute-force Vyos credentials	Vyos Routing VNF	V_{21}: Routing VNF - VyOS Privilege escalation via sudo pppd for operator users	VNF Guest VMs	V_{31}: Privilege escalation through bpf verifier (kernel oriented)	OSM NFVO
V_{12}: SQL Injection RFI, LFI, RCE	Vertical Applications (e.g. DVWA)	V_{12}: docker escape using waitid function (docker bypass)	Vertical Apps Guest VMs	V_{32}: Privilege escalation to root via "sudoedit -s" (kernel oriented)	OSM NFVO

Next, in Figure 9, we organise the qualitative network characteristics indicated in Table 2 in a better context in order to illustrate a possible propagation of a cyber attack across the different vulnerabilities. While this is clearly a partial view of a 5G network, it presents the necessary elements in line with the assumptions of Section 3, and, thus, facilitates the process of demonstrating the application potential of the APILA framework.

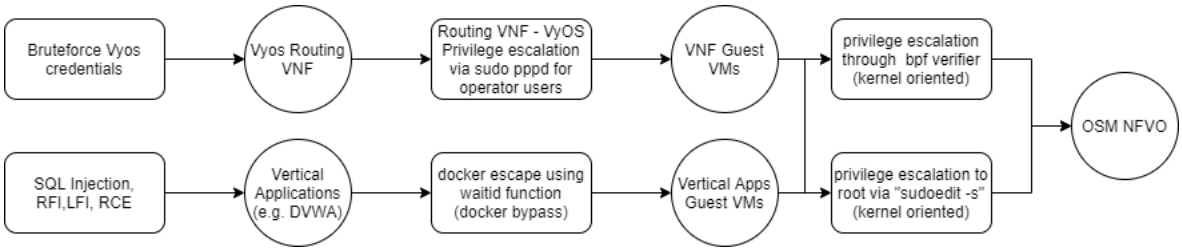

Figure 9: Attack graph representing the attacker actions in a vulnerable artificial 5G infrastructure.

In order to carry out quantitative risk assessment for a network similar to the one of Figure 9, we must make assumptions about key parameters. The parameter values indicated in Table 3 reflect the required input for **i.** asset pricing, involving the evaluation of the impact of a cyber attack for each asset of the network (K_i) and the determination of the associated PV, and ii. impact loss analysis, which is

reflected in the calculation of relevant risk metrics outlined in Table 4. Thus, we will demonstrate the implications of exploitation hardness, which, as indicated in (1) and demonstrated in Scenarios 1 and 2, is not involved in the calculation of K_i, yet, as indicated in (2), it is critical for evaluating its PV.

Table 3: Parameter values and asset pricing.

	Baseline Parameters			**Scenario 1**		
	Phase (i)			Phase (i)		
Parameter	$i=1$	$i=2$	$i=3$	$i=1$	$i=2$	$i=3$
λ_i	-	-	-	2	4	6
A_i	1.5	2	2.25	1.5	2	2.25
R_i	0.25 0.75	0.4 0.6	0.65 0.35	0.25 0.75	0.4 0.6	0.65 0.35
S_i	0.45 0.35	0.24 0.63	0.44 0.23	0.45 0.35	0.24 0.63	0.44 0.23
K_i	0.5625	0.9480	0.9163	0.5625	0.9480	0.9163
	Scenario 2			**Scenario 3**		
	Phase (i)			Phase (i)		
Parameter	$i=1$	$i=2$	$i=3$	$i=1$	$i=2$	$i=3$
λ_i	1	2	3	1	2	3
A_i	1.5	2	2.25	1.5	2	2.25
R_i	0.25 0.75	0.4 0.6	0.65 0.35	0.35 0.65	0.6 0.4	0.65 0.35
S_i	0.45 0.35	0.24 0.63	0.44 0.23	0.55 0.35	0.24 0.7	0.44 0.23
K_i	0.5625	0.9480	0.9163	0.9375	0.9480	0.5498

Based on these parameter values, we can analyse how the risk exposure of the network increases as the attack progresses from one asset to the next. Note that although Figure 9 presents a realistic network of vulnerabilities, aspects of propagation are not particularly pronounced. Therefore, we abstract slightly in Figure 10 in order to illustrate the application potential of the model in a somewhat generalised context. This is implied by the values of R_i being less than one, and, thus, unlike Figure 10, the transition from V_{11} : {Bruteforce Vyos credentials} to V_{21} : {Routing VNF - VyOS Privilege escalation via suddo pppd for operator users} is not certain. Note also that for ease of exposition we omit the state of the attack following the exploitation of a vulnerability as it is not relevant for risk assessment.

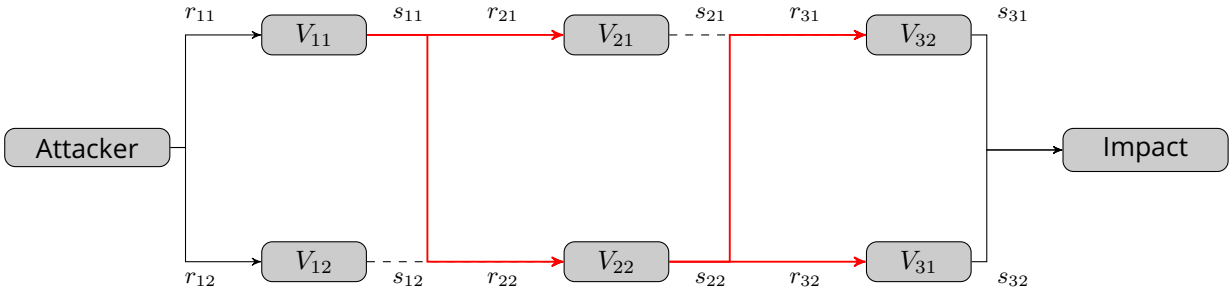

Figure 10: High-level attack graph representing the attacker actions in a vulnerable artificial 5G infrastructure.

Additionally, the different scenarios in Table 3 are designed to demonstrate the importance of (increasing) *exploitation hardness*, and emphasise the implications of the likelihood of successfully compromising a vulnerability for estimating the impact of a cyber attack. Specifically, under a given network topology, the objective of each scenario is outlined below:

- **Scenario 1:** demonstrate how accounting for *exploitation hardness* leads to a lower expected impact.
- **Scenario 2:** emphasise the implications of *exploitation hardness* by allowing for marginal decrease in the values of λ_i.
- **Scenario 3:** demonstrate the impact of a *ceteris paribus* increase in R_i, S_i.

Figure 11 illustrates the distribution of the PV of the impact of a security breach on each asset of the network based on the parameter values of Table 3.

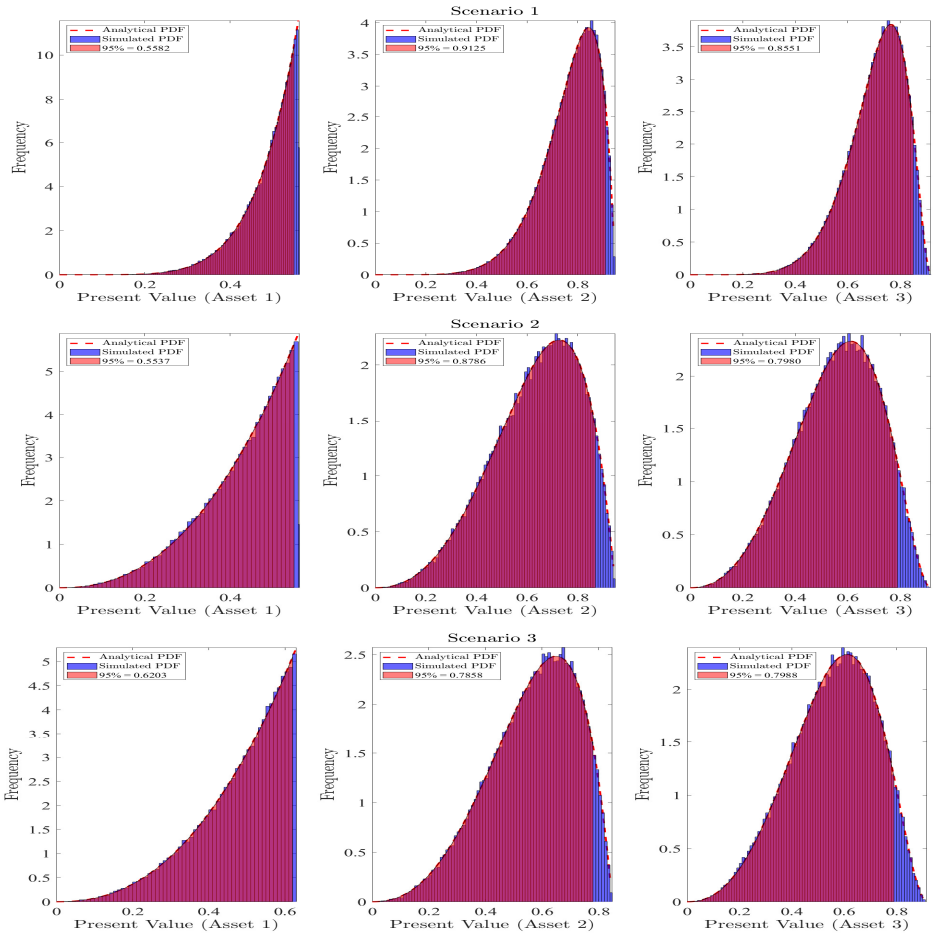

Figure 11: Distribution of the PV of the impact for each asset of the network following a security breach.

For each scenario we observe that:

- **Scenario 1**: A *ceteris paribus* increase in λ_i lowers the expected time required to exploit a vulnerability, and, in turn, raises the expected impact of the security breach.

  Note that this demonstrates the implications of discounting for the value of the expected impact and emphasises the contribution of the DCF method. Indeed, since the time required to exploit a vulnerability is assumed to be exponentially distributed, i.e. $T_i \sim Exp(\lambda_i)$, its expected value is $\mathbb{E}[T_i] = \frac{1}{\lambda_i}$.

- **Scenario 2**: Building upon Scenario 1, we demonstrate here how an increase in *exploitation hardness*, resulting from a decrease in λ_i, lowers the PV of the impact.

  The contribution of this result is to demonstrate how, under certain assumptions, we can quantify the implications of implementing mitigation measures to safeguard vulnerabilities.

- **Scenario 3**: The specific network topology in Figure 10 facilitates attacks on vulnerabilities (V_{11} and V_{22}) that offer greater flexibility over the propagation across the network. Hence, it is plausible to consider the implications of an increase in r_{11} and r_{22}, in terms of its effect on the expected impact.

In line with Figure 11, a list of risk metrics is also summarised in Table 4. Specifically, under each scenario, we indicate key features of the distribution of the PV of K_i i.e. the expectation, the variance, as well as the VaR. To emphasise the implications of lower λ_i (greater exploitation hardness), we indicate its impact in terms of the percentage change in the expected impact and the VaR. In line with intuition, lower exploitation hardness implies that the time required to exploit a vulnerability is shorter, which raises the expected impact of the cyber attack by narrowing the time interval by which it is discounted. This is demonstrated in Scenario 1, where we observe that **i.** accounting for this aspect of a cyber attack the expected impact demonstrates a reduction compared to the baseline scenario, where exploitation hardness is ignored, whereas, **ii.** compared to Scenario 2, where the value of λ_i is lower for all assets, the expected impact reduces even further. The significance of this result is emphasised in the percentage change (where each Scenario is compared to the previous one) in the expected impact and VaR that, in certain cases, is particularly pronounced.

Table 4: Impact loss analysis.

	Baseline Scenario			Scenario 1		
	Asset 1	**Asset 2**	**Asset 3**	**Asset 1**	**Asset 2**	**Asset 3**
Expected Impact	0.5625	0.9480	0.9163	0.4891	0.7668	0.7059
Variance	-	-	-	0.0041	0.0131	0.0123
VaR	-	-	-	0.5581	0.9126	0.8551
% Change in Ex. Impact	-	-	-	-13.05%	-19.11%	-22.96%
	Scenario 2			**Scenario 3**		
	Asset 1	**Asset 2**	**Asset 3**	**Asset 1**	**Asset 2**	**Asset 3**
Expected Impact	0.4327	0.6341	0.5572	0.4846	0.5672	0.5572
Variance	0.0105	0.0300	0.0259	0.0132	0.0240	0.0259
VaR	0.5539	0.8785	0.7988	0.6205	0.7862	0.7990
% Change in Ex. Impact	-11.53%	-17.31%	-21.07%	11.99%	-10.55%	0%
% Change in VaR	10.22%	-10.51%	-6.58%	12.02%	-10.51%	-0.025%

Note that each one of the risk metrics in Table 4 can not only be used for the purpose of impact loss analysis, but, in addition, as we will also demonstrate in D5.4, they can be utilised to formulate objective functions that can be optimised to determine the optimal set of mitigation measures subjective to different constraints. Specifically, the contribution of deriving both the expectation of the PV of the impact and the VaR is that we may now formulate a decision making framework that accounts for different risk preferences.

9 CONCLUSIONS

Efficient cybersecurity risk management relies on managerial strategies that are responsive to the various uncertainties associated with cyber attacks. The need for such strategies becomes particularly pronounced considering the critical impact that cyber attacks may have on organisations and the often very limited time to make executive decisions. Hence, risk management within the area of the cyber security is a considerably delicate task, since the presence of uncertainties raises the incentive to postpone decisions, and, in turn, the value of waiting, which is often a luxury that cannot be afforded.

In this report, we take into account the serial nature of a cyber attack as well as key underlying uncertainties, and develop an analytical framework to: **i.** evaluate the risk exposure of an organisation; and **ii.** develop risk metrics that will serve as optimisation objectives for the optimal selection of mitigation measures in D5.4. Thus, the contribution of our framework is that it extends the traditional DCF approach beyond a static context in order to demonstrate its application potential within a more complex cyber security contact that combines asset valuation and risk management.

Specifically, we derive the expected present value of the cost an organisation incurs following a cyber attack, taking into account the uncertainty in the time an attacker requires to exploit each vulnerability of the 5G network. Doing so, we derive analytical expressions for the distribution of the cost of a cyber attack, and, in turn, we produce risk measures such as the VaR and the CVaR, that can be used to gauge the level of risk exposure. To demonstrate the novelty of our model, we analyse the economic implications of a cyber attack by developing a case study based on a 5G network.

Thus, the contribution of the risk assessment framework is that it provides a critical building block to a decision support tool that will be developed in D5.4. The latter represents the optimisation part of the analysis, where we develop variations of the set cover and knapsack problem in order to optimise the set of controls that can be implemented to mitigate the impact of a cyber attack.

10 APPENDIX

10.1 LIST OF ASSETS

ID	Name	Description	Vulnerabilities	Value
A1	OpenLTE-Virtual-EPC-Core	Implements the Radio Resource Control signalling	V10,V11	M
A2	LTE-Guest-VMs	Linux-based VMs that are used for hosting virtualized LTE components	V1,V2	M
A3	OpenIMS	An open source implementation of LTE-IMS		M
A4	eNodeB(SDR/USRP)	The attachment interface of LTE	V15	M
A5	Hypervisor1-KVM	Raw compute resources based on KVM hypervisor that are used during slicing	V5	M
A6	Hypervisor2-ESXI	Raw compute resources based on ESXI hypervisor that are used during slicing	V4	M
A7	OSM NFVO	Open Source Mano - Network Function Virtualization Orchestrator	V15	M
A8	Vyos Routing VNF	Vyos Open source routing VNF used during slice generation	V6	H
A9	Openstack VIM	The base Virtualized Infrastructure Manager	V9	M
A10	Open5G-SBA-NetworkResourceManagement	An open source reference implementation of the Network Resource Management components of the 5G SBA		M
A11	Open5G-SBA-Signalling	An open source reference implementation of the Signalling components of the 5G SBA	V12	M
A12	Open5G-SBA-Policy	An open source reference implementation of the Policy enforcement components of the 5G SBA		M
A13	Open5G-SBA-IMSCore	An open source reference implementation of the IMS components of the 5G SBA	V15	M
A14	Open5G-SBA-PacketController	An open source reference implementation of the Packet controller components of the 5G SBA		M
A15	Open5G-SBA-SubscriberManagement	An open source reference implementation of the subscriber management components of the 5G SBA	V13	H
A16	Vertical Applications (e.g. DVWA)	It represents any (layer-7) vulnerable component that offers IP-based services to UEs	Layer-7-Vulns	M
A17	UE	The user equipment		M
A18	VNF Guest VMs	Linux-based VMs that are used for hosting virtualized VNFs	V1,V2	M
A19	5G SBA Guest VMs	Linux-based VMs that are used for hosting virtualized SBA components	V1,V2	M
A20	Vertical Apps Guest VMs	Linux-based VMs that are used for hosting vertical application containers	V1,V2	M
A21	Vertical Apps Containers	The containers that isolate the vertical applications	V3	M
A22	GNodeB(SDR/USRP)	The attachment interface of 5G (in a standalone version)	V8,V14	M

Figure 12: Indicative list of assets.

10.2 LIST OF VULNERABILITIES

ID	Name	Formal Identifier (if existing)
V1	privilege escalation to root via "sudoedit -s" (kernel oriented)	CVE-2021-3156
V2	privilege escalation through bpf verifier (kernel oriented)	CVE-2020-8835
V3	docker escape using waitid function (docker bypass)	CVE-2017-5123
V4	remote code execution using OpenSLP (hypervisor takeover from external entity) (host to guest)	CVE-2020-3992
V5	EPYC escape (guest to host escape for KVM)	CVE-2021-29657
V6	Routing VNF - VyOS Privilege escalation via sudo pppd for operator users	CVE-2018-18556
V7	Attacking the SDN Interface of an OSS - SQL injection in the component database(SQLite) without authenticating to the controller or SDNInterfaceapp	CVE-2018-1132
V8	WiFi - dictionary attack	CVE-2019-12941, CVE-1999-1152, CVE-2001-1291, CVE-2001-0395, CVE-2001-1339, CVE-2002-0628
V9	Remote Code Execution	CVE-2020-26943
V10	RRC IMSI catcher	
V11	UE Denial Service (OpenLTE)	
V12	SBA null policy	
V13	SBA key retrival (non integrity)	
V14	Unencrypted PWS	
Layer-7-Vulns	SQL Injection, RFI,LFI	
V15	weak credentials, bruteforce attack	

Figure 13: Indicative list of vulnerabilities.

10.3 PHASE 1

The general expression of the cdf of the PV of K_1 is described in (35).

$$\begin{aligned}\Theta_{U_1}(u_1) &= \mathbb{P}\left(K_1 e^{-\rho\tau_1} \leq u_1\right) \\ &= \mathbb{P}\left(\tau_1 \geq \frac{1}{\rho}\ln\left(\frac{K_1}{u_1}\right)\right) \\ &= 1 - \mathbb{P}\left(\tau_1 \leq \frac{1}{\rho}\ln\left(\frac{K_1}{u_1}\right)\right) \\ &= 1 - \Phi_{W_1}\left(\frac{1}{\rho}\ln\left(\frac{K_1}{u_1}\right)\right) \end{aligned} \tag{35}$$

Note that (35) allows any assumptions about the distribution of T_1. However, for ease of exposition, we will assume here that $T_1 \sim \exp(\lambda_1)$. Thus, the cdf of T_1 is $\Phi_{T_1}(\tau_1) = 1 - \exp\{\lambda_1\}$, and, consequently, the cdf and pdf of the PV of K_1 are described in (36) and (37), respectively.

$$\Theta_{U_1}(u_1) = 1 - 1 + e^{-\frac{\lambda_1}{\rho}\ln\left(\frac{K_1}{u_1}\right)} = \left(\frac{K_1}{u_1}\right)^{-\lambda_1\rho^{-1}} \tag{36}$$

$$\theta_{U_1}(u_1) = \frac{\lambda_1}{\rho} K_1^{-\frac{\lambda_1}{\rho}} \cdot u_1^{\frac{\lambda_1}{\rho}-1} \tag{37}$$

Next, having derived the analytical expression for the distribution of U_1, we can proceed with the derivation of the main moments

$$\mu_1 = \int_0^{K_1} z_1 \frac{\lambda_1}{\rho} K_1^{-\frac{\lambda_1}{\rho}} \cdot u_1^{\frac{\lambda_1}{\rho}-1} du_1 = \frac{\lambda_1}{\lambda_1+\rho} K_1 \tag{38}$$

$$\sigma_1^2 = \mathbb{E}\left[U_1^2\right] - \mathbb{E}\left[U_1\right]^2 = \left[\frac{\lambda_1}{\lambda_1+2\rho} - \left(\frac{\lambda_1}{\lambda_1+\rho}\right)^2\right] K_1^2 \tag{39}$$

$$\gamma_1 = \frac{\mathbb{E}\left[U_1^3\right] - 3\mu_1\sigma_1^2 - \mu_1^3}{\sigma_1^6} \tag{40}$$

$$\delta_1 = \frac{\mathbb{E}\left[\left(U_1-\mu_1\right)^4\right]}{\left[\mathbb{E}\left[\left(U_1-\mu_1\right)^2\right]\right]^2} \tag{41}$$

By definition, $\mathrm{VaR}_\xi(X) = -\inf\{v \in \mathbb{R} : \mathbb{P}(X \leq v) > \xi\}$ evaluates the left tail of a loss random variable X, while $\mathrm{CVaR}_\xi(X)$ is the expectation of X given that it is less than $\mathrm{VaR}_\xi(X)$. However, since we are not considering the distribution of the overall profits, but only the distribution of the impact of a cyber attack, we adopt this general definition of VaR to our context. Specifically, with the closed-from

expression of $\Theta_{U_1}(u_1)$ as specified in (36), we can obtain the analytical expression of VaR as follows:

$$\begin{aligned}
\mathrm{VaR}_{\xi}(U_1) &= \sup\{u_1 : \mathbb{P}(U_1 \geq u_1) > \xi\} \\
&= \sup\{u_1 : 1 - \mathbb{P}(U_1 \leq u_1) > \xi\} \\
&= \sup\left\{u_1 : 1 - \left(\frac{u_1}{K_1}\right)^{\frac{\lambda_1}{\rho}} > \xi\right\} \\
&= \sup\left\{u_1 : K_1(1-\xi)^{-\frac{\lambda_1}{\rho}} < u_1\right\} \\
&= K_1(1-\xi)^{-\frac{\lambda_1}{\rho}}
\end{aligned}$$

Based on the expression of VaR, the expression of CVaR is:

$$\mathrm{CVaR}_{\xi}(U_1) = \frac{1}{p}\int_0^p \mathrm{VaR}_{\xi}(U_1)dq. \tag{42}$$

10.4 PHASE n

Next, we determine the CDF of $U_n = k_n e^{-rW_n}$, where $W_n = T_1 + T_2 + \cdots + T_n$. For a general distribution function $\Phi_{W_n}(w_n)$ we have:

$$\Theta_{U_n}(u_n) = 1 - \Phi_{W_n}\left(\frac{1}{r}\ln\left(\frac{k_n}{u_n}\right)\right) \tag{43}$$

Depending on the CDF of W_n, we can derive a specific expression for the distribution of the U_n. Here, we assume that each T_i follows an exponential distribution with parameter λ_i.

Proof of Proposition 3

$\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_n$

In this case, $W_n \sim Hypo(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and the CDF and PDF of W_n are described in (44) and (45), respectively.

$$\Phi_{W_n}(w_n) = \sum_{i=1}^{n}\left[1 - e^{-\lambda_i w_n}\right]\prod_{j\neq i}\frac{\lambda_j}{\lambda_j - \lambda_i} \tag{44}$$

$$\phi_{W_n}(w_n) = \sum_{i=1}^{n}\lambda_i e^{-\lambda_1 w_n}\prod_{j\neq i}\frac{\lambda_j}{\lambda_j - \lambda_i} \tag{45}$$

Hence, the CDF U_n is obtained by setting $w_n = \frac{1}{r}\ln\left(\frac{k_n}{u_n}\right)$ in (44) and then substituting (44) into (43).

$$\Theta_{U_n}(u_n) = 1 - \sum_{i=1}^{n}\left[1 - \left(\frac{u_n}{k_n}\right)^{\frac{\lambda_i}{r}}\right]\prod_{j\neq i}\frac{\lambda_j}{\lambda_j - \lambda_i} \quad (46)$$

$$\theta_{U_n}(u_n) = \sum_{i=1}^{n}\left[\frac{\lambda_i}{r}\left(\frac{u_n}{k_n}\right)^{\frac{\lambda_i}{r}-1}\frac{1}{k_n}\right]\prod_{j\neq i}\frac{\lambda_j}{\lambda_j - \lambda_i} \quad (47)$$

■

$\lambda_i = \lambda,\ \forall i = 1, \ldots, n$

Now, $W_n \sim Erlang(n, \lambda)$, and, therefore, the CDF and PDF are indicated in (49) and (48), respectively.

$$\Phi_{W_n}(w_n) = 1 - \sum_{i=0}^{n-1}\frac{1}{i!}e^{-\lambda w_n}(\lambda w_n)^i \quad (48)$$

$$\phi_{W_n}(w_n) = \lambda^2 w_n e^{-\lambda w_n} \quad (49)$$

The CDF and PDF U_n is:

$$\Theta_{U_n}(u_n) = e^{-\lambda w_n}\sum_{i=0}^{n-1}\frac{(\lambda w_n)^i}{i!},\ \ w_n = \frac{1}{r}\ln\left(\frac{k_n}{u_n}\right) \quad (50)$$

$$\theta_{U_n}(u_n) = \frac{1}{(n-1)!}\left(\frac{\lambda}{r}\right)^n\left(\frac{u_n}{k_n}\right)^{\frac{\lambda}{r}-1}\frac{1}{k_n}\left(\ln\frac{k_n}{u_n}\right)^{n-1} \quad (51)$$

The mean and variance of the NPV of the arbitrary n_{th} phase is described in (52) and (53), respectively. Notice that an increase in n lowers the expected NPV of the cost, which reflects the effect of discounting.

$$\mu_n = \left(\frac{\lambda}{\lambda + r}\right)^n k_n \quad (52)$$

$$\sigma_n^2 = \left[\left(\frac{\lambda}{\lambda + 2r}\right)^n - \left(\frac{\lambda}{\lambda + r}\right)^{2n}\right]k_n^2 \quad (53)$$

■

References

[1] D2.7 - SPIDER platform reference architecture – Final version.

[2] D5.1 - Continuous risk analysis: models and assessment engine - initial version.

[3] D5.4 - An empirical decision-support framework for econometric analysis of cyber risk and investment.

[4] D5.7 - SPIDER cybersecurity investment component – final version.

[5] D7.4 - Cybersecurity investment decision support pilot.

[6] Grant Agreement NUMBER 833685 - SPIDER.

[7] Simaan M AbouRizk, Daniel W Halpin, and James R Wilson. Visual Interactive Fitting of Beta Distributions. *Journal of Construction Engineering and Management*, 117(4):589–605, 1991.

[8] Christopher Alberts and Audrey Dorofee. Octave criteria. Technical Report CMU/SEI-2001-TR-016, CERT, October 2001.

[9] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security economics and the internal market. https://www.enisa.europa.eu/publications/archive/economics-sec/at_download/fullReport.

[10] Florian Arnold, Holger Hermanns, Reza Pulungan, and Mariëlle Stoelinga. Time-dependent analysis of attacks. In *International Conference on Principles of Security and Trust*, pages 285–305. Springer, 2014.

[11] Michel Benaroch. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research*, 29(2):315–340, 2018.

[12] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56:1–27, 2016.

[13] Stefan Creemers. Minimizing the expected makespan of a project with stochastic activity durations under resource constraints. *Journal of Scheduling*, 18(3):263–273, 2015.

[14] Stefan Creemers. Moments and distribution of the net present value of a serial project. *European Journal of Operational Research*, 267(3):835–848, 2018.

[15] Avinash K Dixit, Robert K Dixit, and Robert S Pindyck. *Investment under uncertainty*. Princeton university press, 1994.

[16] Ashutosh Dutta and Ehab Al-Shaer. Cyber defense matrix: a new model for optimal composition of cybersecurity controls to construct resilient risk mitigation. In *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, pages 1–2, 2019.

[17] ENISA. Incentives and barriers of the cyber insurance market in europe. http://goo.gl/BtNyj4, 2012.

[18] Alison Etheridge and Martin Baxter. *A course in financial calculus*. Cambridge University Press, 2002.

[19] Andrew Fielder, Sandra König, Emmanouil Panaousis, Stefan Schauer, and Stefan Rass. Risk assessment uncertainties in cybersecurity investments. *Games*, 9(2):34, 2018.

[20] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23, 2016.

[21] Mandiant Services FireEye. *M-Trends 2020 Special Report*, 2020 (accessed October 8, 2020).

[22] Roger Flage, Terje Aven, Enrico Zio, and Piero Baraldi. Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. *Risk analysis*, 34(7):1196–1207, 2014.

[23] Daniel Geer, Kevin Soo Hoo, and Jaquith Andrew. Information security: Why the future belongs to the quants. *IEEE Security & Privacy*, 1(2):32–40, 2003.

[24] A. Lawrence Gordon, P. Martin Loeb, and Tashfeen Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, 2003.

[25] Lawrence A Gordon, Martin P Loeb, William Lucyshyn, and Lei Zhou. Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, 1(1):3–17, 2015.

[26] Richard Harang and Alexander Kott. Burstiness of intrusion detection process: Empirical evidence and a modeling approach. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 12(10), 2017.

[27] Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison Wesley, 2007.

[28] A. Paul Jomon and Wang Xinfang. Socially optimal it investment for cybersecurity. *Decision Support Systems*, 122:113069, 2019.

[29] Michael E Kuhl, Natalie M Steiger, Emily K Lada, Mary Ann Wagner, and James R Wilson. Introduction to Modeling and Generating Probabilistic Input Processes for Simulation. In *Proceedings of the 2006 Winter Simulation Conference*, pages 19–35. IEEE, 2006.

[30] Aron Laszka, Mark Felegyhazi, and Levente Buttyan. A survey of interdependent information security games. *ACM Computing Surveys (CSUR)*, 47(2):1–38, 2014.

[31] Yee Wei Law, Tansu Alpcan, and Marimuthu Palaniswami. Security games for risk minimization in automatic generation control. *IEEE Transactions on Power Systems*, 30(1):223–232, 2015.

[32] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 24:35–61, 2017.

[33] Srimathy Mohan, Mohan Gopalakrishnan, H Balasubramanian, and A Chandrashekar. A lognormal approximation of activity duration in PERT using two time estimates. *Journal of the Operational Research Society*, 58(6):827–831, 2007.

[34] Amirreza Niakanlahiji, Jinpeng Wei, Md Rabbi Alam, Qingyang Wang, and Bei-Tseng Chu. Shadowmove: A stealthy lateral movement strategy. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 559–576, 2020.

[35] Thomas R Peltier. *Information security risk analysis*. CRC press, 2005.

[36] Chen Peng, Maochao Xu, Shouhuai Xu, and Taizhong Hu. Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, 44(14):2534–2563, 2017.

[37] Chen Peng, Maochao Xu, Shouhuai Xu, and Taizhong Hu. Modeling multivariate cybersecurity risks. *Journal of Applied Statistics*, 45(15):2718–2740, 2018.

[38] Niels Provos, Markus Friedl, and Peter Honeyman. Preventing privilege escalation. In *USENIX Security Symposium*, 2003.

[39] Terry R Rakes, Jason K Deane, and Loren Paul Rees. It security planning under uncertainty for high-impact events. *Omega*, 40(1):79–88, 2012.

[40] T Mercuri Rebecca. Analyzing security costs. *Communications of the ACM*, 46(6):15–18, 2003.

[41] Ronald S Ross. Guide for conducting risk assessments. Technical report, 2012.

[42] McEvilley Michael Ross Ron and Oren Janet. Systems security engineering, considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. *NIST Special Publication 800-160*, 1, 2016.

[43] Tadeusz Sawik. Selection of optimal countermeasure portfolio in it security planning. *Decision Support Systems*, 55(1):156–164, 2013.

[44] M Sheldon, Ross. *Introduction to Probability Models*. Academic press, 2010.

[45] Fabrizio Smeraldi and Pasquale Malacaria. How to spend it: optimal investment for cyber security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity*, pages 1–4, 2014.

[46] Wes Sonnenreich, Jason Albanese, and Bruce Stout. Return on security investment (rosi)-a practical quantitative model. *Journal of Research and practice in Information Technology*, 38(1):45–56, 2006.

[47] Dan Trietsch, Lilit Mazmanyan, Lilit Gevorgyan, and Kenneth R Baker. Modeling activity times by the Parkinson distribution with a lognormal core: Theory and validation. *European Journal of Operational Research*, 216(2):386–396, 2012.

[48] Paul Voigt and Axel Von dem Bussche. The EU general data protection regulation (GDPR). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[49] Jingguo Wang, Aby Chaudhury, and H Raghav Rao. Research note—a value-at-risk approach to information security investment. *Information Systems Research*, 19(1):106–120, 2008.

[50] Michael E Whitman and Herbert J Mattord. *Principles of information security*. Cengage Learning, 2011.

[51] Kaiyue Zheng, Laura A Albert, James R Luedtke, and Eli Towle. A budgeted maximum multiple coverage model for cybersecurity planning and management. *IISE Transactions*, 51(12):1303–1317, 2019.

[52] Quanyan Zhu and Stefan Rass. On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats. *IEEE Access*, 6:13958–13971, 2018.

[53] Saman A. Zonouz, Himanshu Khurana, William H. Sanders, and Timothy M. Yardley. Rre: A game-theoretic intrusion response and recovery engine. In *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pages 439–448, 2009.