Mathematical Study of Advanced Persistent Threat (APT) Hunting Techniques

Argyrios Alexopoulos[1] and Nicholas J. Daras[2]

Abstract

The paper documents, based mainly on **[3]-[6]** published papers where a consistent mathematical description of cyberspace and various types of Cyber-Attacks and protection measures is presented, a holistic mathematical approach to a rigorous description of Advanced Persistent Threat (APT) actors' modus operandi through various Cyber Kill Chain stages **[2]**. After defining the various elements of Cyber-Attacks we propose some techniques of tracking the modus operandi of the most sophisticated and non-linear cyber actors, the Advanced Persistent Threat actors that are usually nation-state or nation-state backed and usually stay for an extended time under defenders' threshold.

Keywords: Mathematical modeling (models of systems), measure theory, complex spaces, valuation of cyber assets, vulnerability of cyber assets, node supervision, germ of cyber-attack, cyber defense, proactive cyber protection, Advanced Persistent Threat (APT) actors, Indication of Compromise (IOC).

1. Introduction

The aim of the present paper is, based on the previous published papers **[3], [4]. [5], [6]** to document a rigorous description of Advanced Persistent Threat (APT) actors' modus operandi through various Cyber Kill Chain stages. To this end, Section 2 recalls in brief the mathematical definition of cyberspace given in **[3]**. Next, in Section 3, we first remind the concepts of valuations and vulnerabilities of the parts of a node

[1] Cyberspace Analyst staff in International Organization, Belgium, E-mail: argyrios.alexopoulos@yahoo.com

[2] Department of Mathematics and Engineering Sciences, Hellenic Military Academy, 166 73, Vari Attikis, Greece, E-mail: ndaras@sse.gr

constituent, and then in sections 4 and 5, based on these two concepts and all necessary elements from **[3]**, **[4], [5],** and **[6]** we describe the means to detect the modus operandi and some TTPs (Tactics, Techniques and Procedures) through 5 scenarios that the most sophisticated cyber actors (APTs) use to evolve cyber complex attacks **[1]**. Identifying these vectors through the Cyber Kill Chain the defenses are straight forward and no value would be added enumerating them.

2. Mathematical definition of cyberspace

A multilayered weighted (finite or infinite) graph $\boldsymbol{\mathcal{X}}$ with $\boldsymbol{N}$ interconnected layers is said to be an $\boldsymbol{N}-$ **cyber-archetype germ**. An $\boldsymbol{e}-$**manifestation** gives a geographical qualifier at each node of $\boldsymbol{\mathcal{X}}$. It is an embedding of $\boldsymbol{\mathcal{X}}$ into a Cartesian product of $\boldsymbol{N}$ complex projective spaces $\mathbb{C}\mathbf{P}^{\boldsymbol{n_k}} \equiv \mathbf{P}(\mathbb{C}^{\boldsymbol{n_k+1}})$, such that all nodes of $\boldsymbol{\mathcal{X}}$ in the $\boldsymbol{k}-$layer, called $\boldsymbol{e}-$**node manifestations**, are illustrated at weighted points of the set $\mathbb{C}\mathbf{P}^{\boldsymbol{n_k}}$ and all directed edges (flows) of $\boldsymbol{\mathcal{X}}$ in the $\boldsymbol{k}-$layer, called $\boldsymbol{e}-$**edge manifestations**, are given by simple weighted edges, i.e. by weighted homeomorphic images of the closed interval $[\mathbf{0}, \mathbf{1}]$ on $\mathbb{C}\mathbf{P}^{\boldsymbol{n_k}}$, so that, for any $\boldsymbol{k} = \mathbf{1}, \mathbf{2}, \dots, \boldsymbol{N}$,

- the end points of each $e-$edge manifestation on $\mathbb{C}\mathbf{P}^{\boldsymbol{n_k}}$ must be images of end points of a corresponding original directed edge of $\boldsymbol{\mathcal{X}}$ in the $\boldsymbol{k}-$layer
- there should not be any $e-$edge manifestation on $\mathbb{C}\mathbf{P}^{\boldsymbol{n_k}}$ derived from directed $e-$edge of $\boldsymbol{\mathcal{X}}$ in the $\boldsymbol{k}-$layer into which belong points of $e-$edge manifestations that are defined by other nodes of $\boldsymbol{\mathcal{X}}$ in the same layer.

The set $\boldsymbol{\mathcal{S}_e} = \boldsymbol{\mathcal{S}_e}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ of $e-$manifestations of $\boldsymbol{N}-$cyber archetype germs is the $\boldsymbol{e}-$ **superclass** in $\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}}$**.** An $\boldsymbol{e}$**—graph category** $\boldsymbol{\mathcal{E}_\mathcal{C}} = \boldsymbol{\mathcal{E}_\mathcal{C}}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ is a category consisting of the class $\boldsymbol{ob}(\boldsymbol{\mathcal{E}_\mathcal{C}})$, whose elements, called $\boldsymbol{e}$**—objects**, are the pairs $\boldsymbol{\mathcal{X}} = (\boldsymbol{V}, \boldsymbol{E}) \in \boldsymbol{\mathcal{S}_e}$, endowed with a class $\boldsymbol{hom}(\boldsymbol{\mathcal{E}_\mathcal{C}})$ of $\boldsymbol{e}$**—morphisms** on $\boldsymbol{ob}(\boldsymbol{\mathcal{E}_\mathcal{C}})$ and an associative binary operation $\circ$ with identity.

Generalizing, one may consider additionally the following other four basic $\boldsymbol{e}$**—categories**: The $\boldsymbol{e}-$**set category** $\boldsymbol{e_{Set}} = \boldsymbol{e_{Set}}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ where the objects are subsets of $\boldsymbol{\mathcal{E}_\mathcal{C}}$, the $\boldsymbol{e}-$**homomorphism category** $\boldsymbol{e_{Hom}} = \boldsymbol{e_{Hom}}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ where the objects are sets of homomorphisms between subsets of $\boldsymbol{e_{Set}}$, the $\boldsymbol{e}-$**group category** $\boldsymbol{e_{Grp}} = \boldsymbol{e_{Gpr}}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ where the objects are the groups of $\boldsymbol{\mathcal{E}_\mathcal{C}}$ and the $\boldsymbol{e}-$**topological category** $\boldsymbol{e_{Top}} = \boldsymbol{e_{Top}}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times \dots \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}})$ where the

objects are topological subcategories of $\boldsymbol{\mathcal{E}_C}$. For reasons of homogenization of symbolism, we will adopt the following common notation $\boldsymbol{\mathcal{W}_e} = \{\boldsymbol{\mathcal{E}_C}, \boldsymbol{e_{Set}}, \boldsymbol{e_{Hom}}, \boldsymbol{e_{Grp}}, \boldsymbol{e_{Top}}\}$. The objects of each e −category $\boldsymbol{W_e} = \boldsymbol{W_e}(\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times ... \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}}) \in \boldsymbol{\mathcal{W}_e}$ will be called $\boldsymbol{e}$ **−manifestations**. An easy **algebraic** structure in the (infinite) set of all these e—manifestations $(\boldsymbol{V}, \boldsymbol{E})$ and simultaneously, a compatible **topological** structure to allow for a detailed analytic study of $\boldsymbol{\mathcal{S}_e}$ is given in **[3]**. Further, **[3]** investigates the possibility of allocating suitable vector weights to all the objects and morphisms of any e −category $\boldsymbol{W_e} \in \boldsymbol{\mathcal{W}_e} = \{\boldsymbol{\mathcal{E}_C}, \boldsymbol{e_{Set}}, \boldsymbol{e_{Grp}}, \boldsymbol{e_{Top}}\}$. Towards this end, we consider two types of vector weights that can be attached to any object and/or morphism of such an e −category: the maximum weight and the square weight. Any such weight will be a point in the positive quadrant of the plane. Taking this into account, any e −category $\boldsymbol{W_e} \in \boldsymbol{\mathcal{W}_e} = \{\boldsymbol{\mathcal{E}_C}, \boldsymbol{e_{Set}}, \boldsymbol{e_{Hom}}, \boldsymbol{e_{Gpr}}, \boldsymbol{e_{Top}}\}$ can be viewed as an **infinite** e −*graph*$(\mathbb{V}, \mathbb{E})$ with *vector weights*, in such a way that the e −nodes in $\mathbb{V}$ are the e −objects $\boldsymbol{X} \in \boldsymbol{ob}(\boldsymbol{W_e})$, while the e −edges in $\mathbb{E}$ are the e −morphisms $\boldsymbol{h} \in \boldsymbol{hom}(\boldsymbol{W_e})$. For such an e −graph $\mathfrak{G}_{\boldsymbol{W_e}}$ corresponding to an e − category $\boldsymbol{W_e} \in \boldsymbol{\mathcal{W}_e}$, the vector weight of the e −node associated to the e −manifestation $\boldsymbol{\mathcal{X}} = (\boldsymbol{V}, \boldsymbol{E}) \in \mathbb{V} \equiv \boldsymbol{ob}(\boldsymbol{W_e})$ is equal to a weight of $\boldsymbol{\mathcal{X}}$. Bearing all this in mind, in **[3]**, we introduced a suitable intrinsic metric $\boldsymbol{d_{W_e}}$ in the set $\boldsymbol{ob}(\boldsymbol{W_e})$ of objects of an e −category $\boldsymbol{W_e}$. The most significant benefits coming from such a consideration can be derived from the definitions of *cyber-evolution* and *cyber-domain*. To do this, we first defined the concept of e—*dynamics*, as a mapping of the form $\mathcal{cy}$: [0,1] → $\left(\boldsymbol{ob}(\boldsymbol{W_e}), \boldsymbol{d_{W_e}}\right)$; its image is an e—*arrangement*. Each point $\mathcal{cy}(\boldsymbol{t}) \in \mathcal{cy}([0,1])$ is an (instantaneous) local e −node manifestation with an interrelated$e$ −edge manifestation. An e −arrangement together with all of its (instantaneous) e—morphisms is an e −*regularization*. The elements of the completion $\overline{\boldsymbol{ob}(\boldsymbol{W_e})}$ of $\boldsymbol{ob}(\boldsymbol{W_e})$ in $\overline{\mathbb{C}\mathbf{P}^{\boldsymbol{n_1}} \times ... \times \mathbb{C}\mathbf{P}^{\boldsymbol{n_N}}}$ are the *cyber-elements*, while the topological space $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ is a *cyber-domain*. With this notation, a continuous e −dynamics $\mathcal{cy}$: $[\mathbf{0}, \mathbf{1}] \rightarrow \left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ is said to be a *cyber-evolutionary path* or simply *cyber-evolution* in the cyber-domain $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$. Its image is said to be a *cyber-arrangement*. A cyber-arrangement together with all of its (instantaneous) cyber-morphisms is called a *cyberspace*.

In view of the above concepts, **[3]** investigates conditions under which an e −regularization may be susceptible of a projective e −limit. It is important to know

if a $e-$*sub*-regularization is projective $e-$system. Subsequently, we defined and discussed the concept of the *length* in a cyber-domain. For the intrinsic cyber-metric $\boldsymbol{d_{W_e}}$, the distance between two cyber-elements is the length of the "shortest cyber-track" between these cyber-elements. The term shortest cyber-track is defined and is crucial for understanding the concept of *cyber-geodesic*. Although every shortest cyber track on a cyber-length space is a cyber-geodesic, the reverse argument is not valid. In fact, *some cyber-geodesics may fail to be shortest cyber-tracks on large scales*. However, since each cyber-domain $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ is a compact, complete metric space, and since for any pair of cyber-elements in $\overline{\boldsymbol{ob}(\boldsymbol{W_e})}$ there is a cyber-evolutionary path of finite length joining them, one can easily ascertain the following converse result: any *pair of two cyber-elements in each cyber-domain* $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ *has a shortest cyber track joining them*. Finally, **[3]** gives a discussion about the *speed* (: *cyber-speed*) of a cyber-evolution and the *convergence* of a sequence of cyber-evolutions.

3. Mathematical description of cyber-attacks

At any moment $\boldsymbol{t}$, a **node** $\boldsymbol{V}$ in the cyber-domain $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ is composed of cyber constituents consisting in devices $\boldsymbol{D_j^{(V)}}$ (:sensors, routing/switching/bridging assets, regulators of information flow, etc) and resources $\boldsymbol{R_k^{(V)}}$ (:services, data, messages etc), the number of which depend potentially from the three geographical coordinates $\boldsymbol{x_1, x_2, x_3}$ and the time $\boldsymbol{t}$. The criticality of the asset management of every node is of high importance since it affects the whole approach. The order of any used quote of devices $\boldsymbol{D_1^{(V)}}$, $\boldsymbol{D_2^{(V)}}$,… and resources $\boldsymbol{R_1^{(V)}}$, $\boldsymbol{R_2^{(V)}}$,… is assumed to be given, pre-assigned and well defined. We will assume uninterruptedly that:

- the potential number of all ***possible*** devices and resources of $\boldsymbol{V}$ is equal to $\boldsymbol{\mathcal{M}_V \gg 0}$ and $\boldsymbol{\mathcal{L}_V \gg 0}$, respectively, and
- the number of $\boldsymbol{V}$'s ***available*** devices and resources is only $\boldsymbol{m_V = m_V}$ and $\boldsymbol{\ell_V = \ell_V(t)}$ respectively, with $\boldsymbol{m_V < \mathcal{M}_V}$ and $\boldsymbol{\ell_V < \mathcal{L}_V}$.

3.1 Valuations and vulnerabilities of parts of a node constituent

Let $\boldsymbol{U}$,$\boldsymbol{V}$ be two nodes in the cyber-domain $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$ and let $\boldsymbol{\mathcal{K}^{(V)}}$ be an available constituent in $\boldsymbol{V}$:

$$\mathcal{K} = \begin{cases} \boldsymbol{D}, if\ the\ constituent\ is\ a\ device, \\ \boldsymbol{R}, if\ the\ constituent\ is\ a\ resource\ element. \end{cases}$$

Obviously, $\mathcal{K}^{(V)}$ may also be viewed as a nonempty collection of a number of elements. It is easy to see that one can make as much finite $\boldsymbol{\sigma}$ −algebras as partitions on $\mathcal{K}^{(V)}$.

Definition 3.1 For every partition $\mathcal{P}$ of $\mathcal{K}^{(V)}$, let us consider a corresponding $\boldsymbol{\sigma}$ −algebra $\mathfrak{U}_{\mathcal{P}}$ of subsets of $\mathcal{K}^{(V)}$as well as a monotonic measure $\boldsymbol{\mu}$ defined on $\mathfrak{U}_{\mathcal{P}}$. Let also $\boldsymbol{Cr_1}, \boldsymbol{Cr_2}, \dots, \boldsymbol{Cr_{\mathfrak{N}}}$ be $\mathfrak{N} = \mathfrak{N}\left(\mathcal{K}^{(V)}, \mathcal{P}\right)$ objective quantifiable criteria for the assessment of the points of $\mathcal{K}^{(V)}$. Denoting by $\boldsymbol{Cr_j}(\boldsymbol{p}) \in \mathbb{R}$ the value of $\boldsymbol{Cr_j}$ on $\boldsymbol{p} \in \mathcal{K}^{(V)}$ at a point $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}) \in \mathbb{R}^3 \times [\boldsymbol{0}, \boldsymbol{1}]$, suppose

1) the functions $\boldsymbol{Cr_j}(\boldsymbol{p})$ are measurable with respect to $\boldsymbol{\mu}$ and
2) a **valuation weight** $\boldsymbol{u_j}(\boldsymbol{p})$ is attributed by (the user(s) of) $\boldsymbol{U}$ to the Criterion $\boldsymbol{Cr_j}$ on $\boldsymbol{p} \in \mathcal{K}^{(V)}$ at $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}) \in \mathbb{R}^4$.

If $\boldsymbol{E} \in \mathfrak{U}_{\mathcal{P}}$ is a part of $\mathcal{K}^{(V)}$and $\mathfrak{n} \leq \mathfrak{N}$, then a **relative valuation of $\boldsymbol{E}$ from the viewpoint (of user(s)) of node $\boldsymbol{U}$** with respect to the $\mathfrak{n}$ criteria $\boldsymbol{Cr_1}, \boldsymbol{Cr_2}, \dots, \boldsymbol{Cr_{\mathfrak{n}}}$ at the spatiotemporal point $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}) \in \mathbb{R}^4$ is any vector

$$\boldsymbol{A}^{(\boldsymbol{U} \twoheadrightarrow \boldsymbol{V})}(\boldsymbol{E}) = \left(\boldsymbol{a_1}^{(\boldsymbol{U} \twoheadrightarrow \boldsymbol{V})}(\boldsymbol{E}), \boldsymbol{a_2}^{(\boldsymbol{U} \twoheadrightarrow \boldsymbol{V})}(\boldsymbol{E}), \dots, \boldsymbol{a_{\mathfrak{n}}}^{(\boldsymbol{U} \twoheadrightarrow \boldsymbol{V})}(\boldsymbol{E})\right)^{\boldsymbol{T}} \in \mathbb{R}^{\mathfrak{n}}$$

where each definite integral

$$\boldsymbol{a_j}^{(\boldsymbol{U} \twoheadrightarrow \boldsymbol{V})}(\boldsymbol{E}) := \int_{\boldsymbol{E}} \boldsymbol{Cr_j}(\boldsymbol{p}) \boldsymbol{u_j}(\boldsymbol{p}) \boldsymbol{d\mu}(\boldsymbol{p}).$$

is the **component valuation of $\boldsymbol{E}$ from the viewpoint (of user(s)) of the node $\boldsymbol{U}$ into the constituent** $\mathcal{K}^{(V)}$at $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t})$. The number $\mathfrak{n}$ is the **dimension of the valuation**. ■

There is a special category of valuations of particular interest, determined in regards to the low degree of "security" of the constituents of the node. The low degree of security is described completely by the concept of vulnerability.

Definition 3.2 For every partition $\mathcal{P}$ of $\mathcal{K}^{(V)}$, let us consider a corresponding $\boldsymbol{\sigma}$ −algebra $\mathfrak{U}_{\mathcal{P}}$ of subsets of $\mathcal{K}^{(V)}$as well as a monotonic measure $\boldsymbol{\lambda}$ defined on $\mathfrak{U}_{\mathcal{P}}$. Let also $\boldsymbol{SCr_1}, \boldsymbol{SCr_2}, \dots, \boldsymbol{SCr_{\mathfrak{M}}}$ be $\mathfrak{M} = \mathfrak{M}\left(\mathcal{K}^{(V)}, \mathcal{P}\right)$ objective quantifiable criteria for the security assessment of the points of $\mathcal{K}^{(V)}$. Denoting by $\boldsymbol{SCr_j}(\boldsymbol{p}) \in \mathbb{R}$ the value of $\boldsymbol{SeCr_j}$ on $\boldsymbol{p} \in \mathcal{K}^{(V)}$ at a spatiotemporal point $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}) \in \mathbb{R}^3 \times [\boldsymbol{0}, \boldsymbol{1}]$, suppose

1) the functions $\boldsymbol{SCr_j}(\boldsymbol{p})$ are measurable with respect to $\boldsymbol{\lambda}$ and

2) a **vulnerability weight** $\boldsymbol{u_j(p)}$ is attributed by (the (user(s) of) node $\boldsymbol{U}$ to the security criterion $\boldsymbol{SCr_j}$ on $\boldsymbol{p} \in \boldsymbol{\mathcal{K}^{(V)}}$ at $\boldsymbol{(x_1, x_2, x_3, t)} \in \mathbb{R}^4$.

If $\boldsymbol{E} \in \boldsymbol{\mathfrak{U}_{\mathcal{P}}}$ is a part of $\boldsymbol{\mathcal{K}^{(V)}}$and $\mathfrak{m} \leq \mathfrak{M}$, then a **relative vulnerability of $\boldsymbol{E}$ from the viewpoint (of the user(s)) of node $\boldsymbol{U}$** with respect to the $\mathfrak{m}$ security criteria $\boldsymbol{SCr_1, SCr_2, \dots, SCr_{\mathfrak{m}}}at\boldsymbol{(x_1, x_2, x_3, t)} \in \mathbb{R}^4$ is any vector

$$\boldsymbol{B^{(U \rightsquigarrow V)}(E) = \left(b_1^{(U \rightsquigarrow V)}(E), b_2^{(U \rightsquigarrow V)}(E), \dots, b_{\mathfrak{m}}^{(U \rightsquigarrow V)}(E)\right)^T} \in \mathbb{R}^m$$

where each definite integral

$$\boldsymbol{b_j^{(U \rightsquigarrow V)}(E) = \int_E SCr_j(p) u_j(p) d\lambda(p).}$$

is the **component vulnerability of $\boldsymbol{E}$ from the viewpoint (of the (user(s)) of the node $\boldsymbol{U}$ into the constituent $\boldsymbol{\mathcal{K}^{(V)}}$** at $\boldsymbol{(x_1, x_2, x_3, t)}$. The number $\mathfrak{m}$ is the **dimension of the vulnerability**. ■

In what follows, a part $\boldsymbol{E}$ of a ***possible*** device $\boldsymbol{D_k^{(V)}}$ or/and resource $\boldsymbol{R_\xi^{(V)}}$ of $\boldsymbol{V}$ that is evaluated from the viewpoint (of the user(s)) of node $\boldsymbol{U}$ may be denoted by $\boldsymbol{fr\left(D_\kappa^{(V)}\right)}$ or/and $\boldsymbol{fr\left(R_\xi^{(V)}\right)}$, respectively $\boldsymbol{(\kappa = 1, 2, \dots, \mathcal{M}_V, \quad \xi = 1, 2, \dots, \mathcal{L}_V)}$. However, to denote both $\boldsymbol{A^{(U \rightsquigarrow V)}\left(fr\left(D_\kappa^{(V)}\right)\right)}$ and $\boldsymbol{A^{(U \rightsquigarrow V)}\left(fr\left(R_\xi^{(V)}\right)\right)}$ we will prefer to use the common notation $\boldsymbol{A_v^{(U \rightsquigarrow V)}}$**:**

$$\boldsymbol{A_v^{(U \rightsquigarrow V)} = \left(a_{1,v}^{(U \rightsquigarrow V)}, \dots, a_{\mathfrak{m},v}^{(U \rightsquigarrow V)}\right)^T =}$$

$$\begin{cases} \boldsymbol{A_U\left(fr\left(D_v^{(V)}\right)\right), if\ v = 1, 2, \dots, \mathcal{M}_V} \\ \boldsymbol{A_U\left(fr\left(R_{v-\mathcal{M}_V}^{(V)}\right)\right)\ if\ v = \mathcal{M}_V + 1, \mathcal{M}_V + 2, \dots, \mathcal{M}_V + \mathcal{L}_V.} \end{cases}$$

Similarly, to denote both $\boldsymbol{B^{(U \rightsquigarrow V)}\left(fr\left(D_\kappa^{(V)}\right)\right)}$, $\boldsymbol{\kappa = 1, 2, \dots, \mathcal{M}_V}$ and $\boldsymbol{B^{(U \rightsquigarrow V)}\left(fr\left(R_\xi^{(V)}\right)\right)}$, $\boldsymbol{\xi = 1, 2, \dots, \mathcal{L}_V}$, we will prefer to adopt the notation

$$\boldsymbol{B_v^{(U \rightsquigarrow V)} = \left(b_{1,v}^{(U \rightsquigarrow V)}, \dots, b_{\mathfrak{m},v}^{(U \rightsquigarrow V)}\right)^T =}$$

$$\begin{cases} \boldsymbol{B_U\left(fr\left(D_v^{(V)}\right)\right), if\ v = 1, 2, \dots, \mathcal{M}_V} \\ \boldsymbol{B_U\left(fr\left(R_{v-\mathcal{M}_V}^{(V)}\right)\right)\ if\ v = \mathcal{M}_V + 1, \mathcal{M}_V + 2, \dots, \mathcal{M}_V + \mathcal{L}_V.} \end{cases}$$

3.2 Cyber-effects and cyber-interactions

We are now in position to proceed towards a description of homomorphisms between cyber nodes. Let $\boldsymbol{U}$,$\boldsymbol{V}$ be two nodes in the cyber-domain $\left(\overline{\boldsymbol{ob}(\boldsymbol{W_e})}, \boldsymbol{d_{W_e}}\right)$. Without loss of generality, we may suppose the numbers $\boldsymbol{\mathcal{M}_V} + \boldsymbol{\mathcal{L}_V}$ and $\boldsymbol{\mathcal{M}_U} + \boldsymbol{\mathcal{L}_U}$ are both enough large, so that $\boldsymbol{\mathcal{k}} \coloneqq \boldsymbol{\mathcal{M}_V} + \boldsymbol{\mathcal{L}_V} = \boldsymbol{\mathcal{M}_U} + \boldsymbol{\mathcal{L}_U}$. We consider the following sets.

1) $\mathfrak{C}^{(fraction)}(\boldsymbol{V}) =$

$$\left\{\left(fr\left(\boldsymbol{D_1^{(V)}}\right), \dots, fr\left(\boldsymbol{D_{\mathcal{M}_V}^{(V)}}\right), fr\left(\boldsymbol{R_1^{(V)}}\right), \dots, fr\left(\boldsymbol{R_{\mathcal{L}_V}^{(V)}}\right)\right): fr\left(\boldsymbol{D_k^{(V)}}\right), fr\left(\boldsymbol{R_\xi^{(V)}}\right) \in \mathfrak{U}_{\mathcal{P}}, \boldsymbol{\kappa} \leq \boldsymbol{\mathcal{M}_V}, \boldsymbol{\xi} \leq \boldsymbol{\mathcal{L}_V}\right\}:$$

the set of ordered columns of possible parts of constituents of $\boldsymbol{V}$;

2) $\boldsymbol{\mathcal{A}_U}\mathfrak{C}^{(fraction)}(\boldsymbol{V}) =$

$$\left\{\left(\boldsymbol{A_1^{(U \rightsquigarrow V)}}, \dots, \boldsymbol{A_{\mathcal{k}}^{(U \rightsquigarrow V)}}\right): \boldsymbol{A_v^{(U \rightsquigarrow V)}} \in \mathbb{R}^{\mathfrak{n}}, \boldsymbol{v} = \boldsymbol{1}, \boldsymbol{2}, \dots, \boldsymbol{\mathcal{k}}\right\} \equiv \mathbb{R}^{\mathfrak{n} \times \mathcal{k}}:$$

the set of ordered columns of relative *valuations* of parts of possible constituents of $\boldsymbol{V}$, from the viewpoint of $\boldsymbol{U}$, over the space time $\mathbb{R}^{\boldsymbol{3}} \times [\boldsymbol{0}, \boldsymbol{1}]$;

3) $\boldsymbol{\mathcal{B}_U}\mathfrak{C}^{(fraction)}(\boldsymbol{V}) =$

$$\left\{\left(\boldsymbol{B_1^{(U \rightsquigarrow V)}}, \dots, \boldsymbol{B_{\mathcal{k}}^{(U \rightsquigarrow V)}}\right): \boldsymbol{B_v^{(U \rightsquigarrow V)}} \in \mathbb{R}^{\mathfrak{n}}, \boldsymbol{v} = \boldsymbol{1}, \boldsymbol{2}, \dots, \boldsymbol{\mathcal{k}}\right\} \equiv \mathbb{R}^{\mathfrak{n} \times \mathcal{k}}:$$

the set of all ordered columns of relative *vulnerabilities* of parts of possible constituents in $\boldsymbol{V}$, from the viewpoint of $\boldsymbol{U}$, over $\mathbb{R}^{\boldsymbol{3}} \times [\boldsymbol{0}, \boldsymbol{1}]$.

Definition 3.3 The triplet

$$\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{P}}(\boldsymbol{V}) = \left(\mathfrak{C}^{(fraction)}(\boldsymbol{V}), \boldsymbol{\mathcal{A}_U}\mathfrak{C}^{(fraction)}(\boldsymbol{V}), \boldsymbol{\mathcal{B}_U}\mathfrak{C}^{(fraction)}(\boldsymbol{V})\right)$$

is called the **cyber-range of $\boldsymbol{V}$ from the viewpoint of (the users of) $\boldsymbol{U}$**. Its elements $\boldsymbol{\mathcal{p}}$ are the (**threefold**) **cyber situations**. Especially, when an Advanced Persistent Threat Hunting is of our interest on node $\boldsymbol{V}$, and given the sophistication of the attack vectors used by these actors, we definitely work on the specific case where $\boldsymbol{U} = \boldsymbol{V}$. In that case the cyber-field $\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{P}}(\boldsymbol{V})$ is the **cyber-purview** of $\boldsymbol{V}$ and is denoted $\boldsymbol{\mathcal{P}^{(self)}} = \boldsymbol{\mathcal{P}^{(self)}}(\boldsymbol{V})$. Its elements are represented by $\widehat{\boldsymbol{\mathcal{p}}}$. With APT actors' TTPs it is not recommended to use the cyber-field $\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{P}}(\boldsymbol{V})$ since the results/conclusions could be misleading.■

Given an ordered set

$$\boldsymbol{FR^{(V)}}: = \left(fr\left(\boldsymbol{D_1^{(V)}}\right), \dots, fr\left(\boldsymbol{D_{\mathcal{M}_V}^{(V)}}\right), fr\left(\boldsymbol{R_1^{(V)}}\right), \dots, fr\left(\boldsymbol{R_{\mathcal{L}_V}^{(V)}}\right)\right)$$

of ordered columns of parts of constituents of $\boldsymbol{V}$, a cyber situation $\boldsymbol{\mathcal{p}}$ on $\boldsymbol{V}$can be viewed as an ordered pair of matrices

$$\boldsymbol{\mathcal{p}} = \left(\mathbb{A}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}, \mathbb{B}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right) = \left(\left(\boldsymbol{a_{i,j}}\right), \left(\boldsymbol{b_{i,j}}\right)\right) \in \mathbb{R}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{R}^{\mathfrak{m}\times\mathfrak{k}}$$

where

$$\mathbb{A}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})} = \left(\boldsymbol{A_1^{(U\rightsquigarrow V)}}, \dots, \boldsymbol{A_{\mathfrak{k}}^{(U\rightsquigarrow V)}}\right) = \left(\boldsymbol{a_{i,j}}\right) = \begin{pmatrix} \boldsymbol{a_{1,1}^{(U\rightsquigarrow V)}} & \cdots & \boldsymbol{a_{1,\mathfrak{k}}^{(U\rightsquigarrow V)}} \\ \vdots & \vdots & \vdots \\ \boldsymbol{a_{\mathfrak{n},1}^{(U\rightsquigarrow V)}} & \cdots & \boldsymbol{a_{\mathfrak{n},\mathfrak{k}}^{(U\rightsquigarrow V)}} \end{pmatrix} \text{ and}$$

$$\mathbb{B}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})} = \left(\boldsymbol{B_1^{(U\rightsquigarrow V)}}, \dots, \boldsymbol{B_{\mathfrak{k}}^{(U\rightsquigarrow V)}}\right) = \left(\boldsymbol{b_{i,j}}\right) = \begin{pmatrix} \boldsymbol{b_{1,1}^{(U\rightsquigarrow V)}} & \cdots & \boldsymbol{b_{1,\mathfrak{k}}^{(U\rightsquigarrow V)}} \\ \vdots & \vdots & \vdots \\ \boldsymbol{b_{\mathfrak{m},1}^{(U\rightsquigarrow V)}} & \cdots & \boldsymbol{b_{\mathfrak{m},\mathfrak{k}}^{(U\rightsquigarrow V)}} \end{pmatrix}.$$

In particular, any purview $\widehat{\boldsymbol{\mathcal{p}}}$ on $\boldsymbol{V}$, can simply be viewed as an ordered pair

$$\widehat{\boldsymbol{\mathcal{p}}} = \left(\widehat{\mathbb{A}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}, \widehat{\mathbb{B}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}\right) = \left(\left(\widehat{\boldsymbol{a}}_{\boldsymbol{i,j}}\right), \left(\widehat{\boldsymbol{b}}_{\boldsymbol{i,j}}\right)\right) \in \mathbb{R}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{R}^{\mathfrak{m}\times\mathfrak{k}}$$

with

$$\widehat{\mathbb{A}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})} = \left(\widehat{\boldsymbol{a}}_{\boldsymbol{i,j}}\right) = \begin{pmatrix} \boldsymbol{a_{1,1}^{(V\rightsquigarrow V)}} & \cdots & \boldsymbol{a_{1,\mathfrak{k}}^{(V\rightsquigarrow V)}} \\ \vdots & \vdots & \vdots \\ \boldsymbol{a_{\mathfrak{n},1}^{(V\rightsquigarrow V)}} & \cdots & \boldsymbol{a_{\mathfrak{n},\mathfrak{k}}^{(V\rightsquigarrow V)}} \end{pmatrix} \text{ and}$$

$$\widehat{\mathbb{B}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})} = \left(\widehat{\boldsymbol{b}}_{\boldsymbol{i,j}}\right) = \begin{pmatrix} \boldsymbol{b_{1,1}^{(V\rightsquigarrow V)}} & \cdots & \boldsymbol{b_{1,\mathfrak{k}}^{(V\rightsquigarrow V)}} \\ \vdots & \vdots & \vdots \\ \boldsymbol{b_{\mathfrak{m},1}^{(V\rightsquigarrow V)}} & \cdots & \boldsymbol{b_{\mathfrak{m},\mathfrak{k}}^{(V\rightsquigarrow V)}} \end{pmatrix}.$$

To simplify our approach, in what follows we will assume that ***the location*** $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}) \in \mathbb{R}^{\boldsymbol{3}}$ ***of V remains constantly fixed***.

Definition 3.4 The **supervision vector of $\boldsymbol{V}$ in the node system** $(\boldsymbol{V}, \boldsymbol{U})$ at a given time moment $\boldsymbol{t} \in [\boldsymbol{0}, \boldsymbol{1}]$ is defined to be the pair

$$(\mathbb{z}, \mathbb{w})(\boldsymbol{t}) = \left(\mathbb{A}_{\boldsymbol{U}\rightarrow\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{A}}_{\boldsymbol{V}\rightarrow\boldsymbol{V}}, \mathbb{B}_{\boldsymbol{U}\rightarrow\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{B}}_{\boldsymbol{V}\rightarrow\boldsymbol{V}}\right)(\boldsymbol{t}) \in \mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}$$

with $\boldsymbol{i} := \sqrt{-\boldsymbol{1}} \in \mathbb{C}$. Especially, the complex matrices $\mathbb{z}$ and $\mathbb{w}$ are called **supervisory perceptions of $\boldsymbol{V}$ in the node system** $(\boldsymbol{V}, \boldsymbol{U})$ at moment $\boldsymbol{t}$. The mapping defined by

$$\boldsymbol{\gamma_V}: [\boldsymbol{0}, \boldsymbol{1}] \to \mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}: \boldsymbol{t} \mapsto \boldsymbol{\gamma_V}(\boldsymbol{t}) = (\mathbb{z}, \mathbb{w})(\boldsymbol{t})$$

is the **supervisory perception curve of $\boldsymbol{V}$ in the node system**$(\boldsymbol{V}, \boldsymbol{U})$ **during the whole of time interval** $[\boldsymbol{0}, \boldsymbol{1}]$. The **supervisory perception domain of $\boldsymbol{V}$ in the node system** $(\boldsymbol{V}, \boldsymbol{U})$ is the range $\boldsymbol{\gamma_V}([\boldsymbol{0}, \boldsymbol{1}])$ of $\boldsymbol{\gamma_V}$, denoted by $\boldsymbol{\gamma_V^*}$.■

Theoretically, each point in the space $\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}$ can be viewed as a supervision vector of $\boldsymbol{V}$ in the system of nodes $\boldsymbol{V}$ and $\boldsymbol{U}$. Since in many cases, it suffices (or is preferable) to use only specific supervisions from the viewpoint of $\boldsymbol{U}$ or $\boldsymbol{V}$:

$(\mathbb{A}_{U\to V}, \mathbb{B}_{U\to V})(t)$ or $(\widehat{\mathbb{A}}_{V\to V}, \widehat{\mathbb{B}}_{V\to V})(t)$ or $(\mathbb{A}_{U\to V}, i\widehat{\mathbb{B}}_{V\to V})(t)$ or $(i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V})(t)$

In our case study and in the context of this paper we assume that an APT actor has already initiated some malicious activity in node V. Therefore, it is constructive to consider the following vector fields on γ_V^* and to use them accordingly, in combination with the other techniques that we consider in this paper, in order to locate and identify the evolved APT vectors and behaviors:

– The vector field $X2$ which assigns to each point

$$(\mathbb{z}, \mathbb{w})(t) = (\mathbb{A}_{U\to V} + i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V} + i\widehat{\mathbb{B}}_{V\to V})(t)$$

of γ_V^* the vector

$$(Im\mathbb{z}, Im\mathbb{w})(t) \equiv (0 + i\widehat{\mathbb{A}}_{V\to V}, 0 + i\widehat{\mathbb{B}}_{V\to V})(t) \in \mathbb{R}^{n\times k} \times \mathbb{R}^{m\times k},$$

i.e., the vector of the *valuations* and *vulnerabilities* of $FR^{(V)}$ at t, considered from the viewpoint of V itself; in subsequently, we may define the vector fields $Y2$ and $Z2$ assigning to each point $(\mathbb{z}, \mathbb{w})(t) = (\mathbb{A}_{U\to V} + i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V} + i\widehat{\mathbb{B}}_{V\to V})(t)$ of γ_V^* the vectors of *valuations* and *vulnerabilities* of $FR^{(V)}$ at t, considered from the viewpoint of V itself:

$$Im\mathbb{z}(t) \equiv \widehat{\mathbb{A}}_{V\to V}(t) \in \mathbb{R}^{n\times k} \text{ and } Im\mathbb{w}(t) \equiv \widehat{\mathbb{B}}_{V\to V}(t) \in \mathbb{R}^{m\times k}.$$

We may also consider combinatorial vector fields, for instance the vector field $X3$ which assigns to each point

$$(\mathbb{z}, \mathbb{w})(t) = (\mathbb{A}_{U\to V} + i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V} + i\widehat{\mathbb{B}}_{V\to V})(t)$$

of γ_V^* the vector

$$(Re\mathbb{z}, Im\mathbb{w})(t) \equiv (\mathbb{A}_{U\to V} + i0, 0 + i\widehat{\mathbb{B}}_{V\to V})(t) \in \mathbb{R}^{n\times k} \times \mathbb{R}^{m\times k},$$

i.e., the vector containing relative *valuations* of $FR^{(V)}$ at t considered from the viewpoint of U and *vulnerabilities* of $FR^{(V)}$at t considered from the viewpoint of V itself, or the vector field $X4$ which assigns to each point

$$(\mathbb{z}, \mathbb{w})(t) = (\mathbb{A}_{U\to V} + i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V} + i\widehat{\mathbb{B}}_{V\to V})(t)$$

of γ_V^* the vector

$$(Im\mathbb{z}, Re\mathbb{w})(t) \equiv (0 + i\widehat{\mathbb{A}}_{V\to V}, \mathbb{B}_{U\to V} + i0)(t).$$

i.e., the vector containing *valuations* of $FR^{(V)}$ at t considered from the viewpoint of V itself and relative *vulnerabilities* of $FR^{(V)}$ at t considered from the viewpoint of U itself.

The concept of supervisory perception curve is a concept that provides a clear overall relative evaluation of a node in time domain and particularly contains the

changes of the quantitative overview on the node. In this sense, the supervisory perception curve could be considered as a concept that provides for the appearance of an action which could lead to changes.

Definition 3.5 A **cyber-activity** of $\boldsymbol{U}$ on $\boldsymbol{V}$ over the time interval $]\boldsymbol{\sigma},\boldsymbol{\tau}[\subset\subset]\mathbf{0},\mathbf{1}[$ is a collection of correspondences from the product $\mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{U})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{V})}$ into the set $\mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{U})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{V})}$:

$$\left(\boldsymbol{\mathcal{G}_t} : \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{U})} \to \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{U})} : \left(\boldsymbol{\gamma_V}(\boldsymbol{t}), \boldsymbol{\delta_U}(\boldsymbol{t})\right) \mapsto \left(\boldsymbol{\gamma_V}(\boldsymbol{t}'), \boldsymbol{\delta_U}(\boldsymbol{t}')\right)\right)_{\boldsymbol{t}\in]\boldsymbol{\sigma},\boldsymbol{\tau}[}$$

$$(\boldsymbol{t}' := \boldsymbol{t} + \Delta\boldsymbol{t} \in]\boldsymbol{\sigma},\boldsymbol{\tau}[).$$

Notice that the case $\Delta\boldsymbol{t} = \mathbf{0}$ is not excluded. A **cyber-interplay** of the ordered cyber pair $(\boldsymbol{V},\boldsymbol{U})$ over the time interval $]\boldsymbol{\sigma},\boldsymbol{\tau}[\subset\subset [\mathbf{0},\infty[$ is an open shift curve

$$\boldsymbol{\mathcal{G}}:]\boldsymbol{\sigma},\boldsymbol{\tau}[\to \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{U})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{U})}:$$

$$\boldsymbol{t} \mapsto \boldsymbol{\mathcal{G}}(\boldsymbol{t}) := \left(\boldsymbol{\gamma_V}(\boldsymbol{t}), \boldsymbol{\delta_U}(\boldsymbol{t}), \boldsymbol{\gamma_V}(\boldsymbol{t}+\Delta\boldsymbol{t}), \boldsymbol{\delta_U}(\boldsymbol{t}+\Delta\boldsymbol{t})\right)$$

$$(\boldsymbol{t}+\Delta\boldsymbol{t} \in]\boldsymbol{\sigma},\boldsymbol{\tau}[).$$

If the cyber-interplay $\boldsymbol{\mathcal{G}}$ is composition of several separate interplays, we say that $\boldsymbol{\mathcal{G}}$ is **sequential**; otherwise is called **elementary**. ■

In that regard to the concept of cyber-activity, we have the concept of cyber-interaction.

Definition 3.6 A **cyber-interaction** between $\boldsymbol{U}$ and $\boldsymbol{V}$ at a given time moment $\boldsymbol{t_0} \in]\boldsymbol{\sigma},\boldsymbol{\tau}[$ is a tetrad

$$\boldsymbol{\mathcal{Z}} = \boldsymbol{\mathcal{Z}}_{(\boldsymbol{U},\boldsymbol{V})}(\boldsymbol{t_0}) = \left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}), (\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}}\right)^{\mathbf{4}}$$

for which there is an associated cyber-activity of $\boldsymbol{U}$ on $\boldsymbol{V}$:

$$\left(\boldsymbol{\mathcal{G}_t} = \boldsymbol{\mathcal{G}}_{\boldsymbol{t}}^{(\boldsymbol{\mathcal{Z}})} : \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{U})} \to \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{V})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{U})} : \left(\boldsymbol{\gamma_V}(\boldsymbol{t}), \boldsymbol{\delta_U}(\boldsymbol{t})\right) \mapsto \left(\boldsymbol{\gamma_V}(\boldsymbol{t}'), \boldsymbol{\delta_U}(\boldsymbol{t}')\right)\right)_{\boldsymbol{t}\in]\boldsymbol{\sigma},\boldsymbol{\tau}[}$$

$$(\boldsymbol{t}' := \boldsymbol{t} + \Delta\boldsymbol{t} \in]\boldsymbol{\sigma},\boldsymbol{\tau}[),$$

such that

$$(\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}) = \boldsymbol{\gamma_V}(\boldsymbol{t_0}) = \left(\mathbb{A}_{\boldsymbol{U}\to\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{A}}_{\boldsymbol{V}\to\boldsymbol{V}}, \mathbb{B}_{\boldsymbol{U}\to\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{B}}_{\boldsymbol{V}\to\boldsymbol{V}}\right) \in \mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}},$$

$$(\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}) = \boldsymbol{\delta_U}(\boldsymbol{t_0}) = \left(\mathbb{A}_{\boldsymbol{V}\to\boldsymbol{U}} + \boldsymbol{i}\widehat{\mathbb{A}}_{\boldsymbol{U}\to\boldsymbol{U}}, \mathbb{B}_{\boldsymbol{V}\to\boldsymbol{U}} + \boldsymbol{i}\widehat{\mathbb{B}}_{\boldsymbol{U}\to\boldsymbol{U}}\right) \in \mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}},$$

$$(\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}) = \boldsymbol{\gamma_V}(\boldsymbol{t}'_{\mathbf{0}}) = \left(\mathbb{A}'_{\boldsymbol{U}\to\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{A}}'_{\boldsymbol{V}\to\boldsymbol{V}}, \mathbb{B}'_{\boldsymbol{U}\to\boldsymbol{V}} + \boldsymbol{i}\widehat{\mathbb{B}}'_{\boldsymbol{V}\to\boldsymbol{V}}\right) \in \mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}},$$

$$(\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}}) = \boldsymbol{\delta_U}(\boldsymbol{t}'_{\mathbf{0}}) = \left(\mathbb{A}'_{\boldsymbol{V}\to\boldsymbol{U}} + \boldsymbol{i}\widehat{\mathbb{A}}'_{\boldsymbol{U}\to\boldsymbol{U}}, \mathbb{B}'_{\boldsymbol{V}\to\boldsymbol{U}} + \boldsymbol{i}\widehat{\mathbb{B}}'_{\boldsymbol{U}\to\boldsymbol{U}}\right) \in \mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}}.\blacksquare$$

Obviously, keeping a fixed supervisory perception $\boldsymbol{\gamma_V(t_0)}$ in the archetype germ $\mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{V})}$and a fixed supervisory perception $\boldsymbol{\gamma_U(t+\Delta t)}$ in the component image germ $\mathbb{G}_{\boldsymbol{t+\Delta t}}^{(\boldsymbol{U})}$, the corresponding cyber-interaction becomes a cyber-effect. And, as we shall see below, proper management of cyber-effects is enough to study cyber navigations. However, in most cases, as in the case of cyber-attacks, it is necessary to consider cyber-interactions. So, because cyber-effects are a partial case of cyber-interactions, we will give a slight priority in the most general context of cyber-interactions.

It is easily verified that the general form of a cyber-interaction is as follows.

$$\boldsymbol{\mathcal{Z}} = \big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\big)$$

$$= \big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\big)(\boldsymbol{t_0})$$

$$= \Bigg(\Bigg(\underbrace{\begin{pmatrix} a_{1,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{1,1}^{(V\rightsquigarrow V)} & \cdots\cdots & a_{1,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ a_{m_V,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{m_V,1}^{(V\rightsquigarrow V)} & & a_{m_V,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{m_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ a_{\mathcal{M}_V,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V,1}^{(V\rightsquigarrow V)} & \cdots\cdots & a_{\mathcal{M}_V,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ a_{\mathcal{M}_V+1,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & a_{\mathcal{M}_V+1,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V+1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ a_{\mathcal{M}_V+\mathcal{L}_V,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V+\mathcal{L}_V,1}^{(V\rightsquigarrow V)} & \cdots\cdots & a_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \end{pmatrix}}_{(\mathbb{z}_1,\mathbb{w}_1)=\boldsymbol{\gamma_V(t_0)}=(\mathbb{A}_{U\rightarrow V}+i\hat{\mathbb{A}}_{V\rightarrow V},\mathbb{B}_{U\rightarrow V}+i\hat{\mathbb{B}}_{V\rightarrow V})\in\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}}\times\mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}}, \underbrace{\begin{pmatrix} b_{1,1}^{(W\rightsquigarrow V)} + i\ \hat{b}_{1,1}^{(V\rightsquigarrow V)} & \cdots\cdots & b_{1,\mathfrak{m}}^{(W\rightsquigarrow V)} + i\ \hat{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ b_{m_V,1}^{(W\rightsquigarrow V)} + i\ \hat{b}_{m_V,1}^{(V\rightsquigarrow V)} & & b_{m_V,\mathfrak{m}}^{(W\rightsquigarrow V)} + i\ \hat{b}_{m_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ b_{\mathcal{M}_V,1}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V,1}^{(V\rightsquigarrow V)} & \cdots\cdots & b_{\mathcal{M}_V,\mathfrak{m}}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ b_{\mathcal{M}_V+1,1}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & b_{\mathcal{M}_V+1,\mathfrak{m}}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ b_{\mathcal{M}_V+\mathcal{L}_V,1}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V+\mathcal{L}_V,1}^{(V\rightsquigarrow V)} & \cdots\cdots & b_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{m}}^{(W\rightsquigarrow V)} + i\ \hat{b}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \end{pmatrix}}_{} \Bigg), \Bigg(\underbrace{\begin{pmatrix} a_{1,1}^{(V\rightsquigarrow W)} + i\ \hat{a}_{1,1}^{(W\rightsquigarrow W)} & \cdots\cdots & a_{1,\mathfrak{n}}^{(V\rightsquigarrow W)} + i\ \hat{a}_{1,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ a_{m_W,1}^{(V\rightsquigarrow W)} + i\ \hat{a}_{m_W,1}^{(W\rightsquigarrow W)} & & a_{m_W,\mathfrak{n}}^{(V\rightsquigarrow W)} + i\ \hat{a}_{m_W,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ a_{\mathcal{M}_W,1}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W,1}^{(W\rightsquigarrow W)} & \cdots\cdots & a_{\mathcal{M}_W,\mathfrak{n}}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ a_{\mathcal{M}_W+1,1}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W+1,1}^{(W\rightsquigarrow W)} & & a_{\mathcal{M}_W+1,\mathfrak{n}}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W+1,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ a_{\mathcal{M}_W+\mathcal{L}_W,1}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W+\mathcal{L}_W,1}^{(W\rightsquigarrow W)} & \cdots\cdots & a_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{n}}^{(V\rightsquigarrow W)} + i\ \hat{a}_{\mathcal{M}_W+\mathcal{L}_W,1}^{(W\rightsquigarrow W)} \end{pmatrix}}_{(\mathbb{z}_2,\mathbb{w}_2)=\boldsymbol{\delta_U(t_0)}=(\mathbb{A}_{V\rightarrow U}+i\hat{\mathbb{A}}_{U\rightarrow U},\mathbb{B}_{V\rightarrow U}+i\hat{\mathbb{B}}_{U\rightarrow U})\in\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}}\times\mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}}, \underbrace{\begin{pmatrix} b_{1,1}^{(V\rightsquigarrow W)} + i\ \hat{b}_{1,1}^{(W\rightsquigarrow W)} & \cdots\cdots & b_{1,\mathfrak{m}}^{(V\rightsquigarrow W)} + i\ \hat{b}_{1,\mathfrak{m}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ b_{m_W,1}^{(V\rightsquigarrow W)} + i\ \hat{b}_{m_W,1}^{(W\rightsquigarrow W)} & & b_{m_W,\mathfrak{m}}^{(V\rightsquigarrow W)} + i\ \hat{b}_{m_W,\mathfrak{m}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ b_{\mathcal{M}_W,1}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W,1}^{(W\rightsquigarrow W)} & \cdots\cdots & b_{\mathcal{M}_W,\mathfrak{m}}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W,\mathfrak{m}}^{(W\rightsquigarrow W)} \\ b_{\mathcal{M}_W+1,1}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W+1,1}^{(W\rightsquigarrow W)} & & b_{\mathcal{M}_W+1,\mathfrak{m}}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W+1,\mathfrak{m}}^{(W\rightsquigarrow W)} \\ \cdots & & \cdots \\ b_{\mathcal{M}_W+\mathcal{L}_W,1}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W+\mathcal{L}_W,1}^{(W\rightsquigarrow W)} & \cdots\cdots & b_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{m}}^{(V\rightsquigarrow W)} + i\ \hat{b}_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{m}}^{(W\rightsquigarrow W)} \end{pmatrix}}_{} \Bigg), \Bigg(\underbrace{\begin{pmatrix} a'^{(W\rightsquigarrow V)}_{1,1} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{1,1} & \cdots\cdots & a'^{(W\rightsquigarrow V)}_{1,\mathfrak{n}} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(W\rightsquigarrow V)}_{m_V,1} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{m_V,1} & & a'^{(W\rightsquigarrow V)}_{m_V,\mathfrak{n}} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V,1} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V,1} & \cdots\cdots & a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V,\mathfrak{n}} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V,\mathfrak{n}} \\ a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,1} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,1} & \cdots\cdots & a'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{n}} + i\ \hat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{n}} \end{pmatrix}}_{(\mathbb{z}'_1,\mathbb{w}'_1)=\boldsymbol{\gamma_V(t'_0)}=(\mathbb{A}'_{U\rightarrow V}+i\hat{\mathbb{A}}'_{V\rightarrow V},\mathbb{B}'_{U\rightarrow V}+i\hat{\mathbb{B}}'_{V\rightarrow V})\in\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}}\times\mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}}, \underbrace{\begin{pmatrix} b'^{(W\rightsquigarrow V)}_{1,1} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{1,1} & \cdots\cdots & b'^{(W\rightsquigarrow V)}_{1,\mathfrak{m}} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(W\rightsquigarrow V)}_{m_V,1} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{m_V,1} & & b'^{(W\rightsquigarrow V)}_{m_V,\mathfrak{m}} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V,1} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V,1} & \cdots\cdots & b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V,\mathfrak{m}} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V,\mathfrak{m}} \\ b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,1} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,1} & \cdots\cdots & b'^{(W\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{m}} + i\ \hat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\mathcal{L}_V,\mathfrak{m}} \end{pmatrix}}_{} \Bigg) \Bigg).$$

$$\underbrace{\left(\begin{pmatrix} a'^{(V\rightsquigarrow W)}_{1,1}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{1,1} & \cdots\cdots & a'^{(V\rightsquigarrow W)}_{1,\mathfrak{n}}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\rightsquigarrow W)}_{m_W,1}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{m_W,1} & & a'^{(V\rightsquigarrow W)}_{m_W,\mathfrak{n}}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{m_W+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\rightsquigarrow W)}_{\mathcal{M}_W,1}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W,1} & \cdots\cdots & a'^{(V\rightsquigarrow W)}_{\mathcal{M}_W,\mathfrak{n}}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+1,\mathfrak{n}} \\ a'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+1,1}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+1,1} & & \cdots \\ \cdots & & a'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{n}}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{n}} \\ a'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,1}+i\ \widehat{a}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,1} & \cdots\cdots & \end{pmatrix}}_{(\mathbb{z}'_2,\mathbb{w}'_2)=\boldsymbol{\delta}_U(t'_0)=(\mathbb{A}'_{V\rightarrow U}+i\widehat{\mathbb{A}}'_{U\rightarrow U},\mathbb{B}'_{V\rightarrow U}+i\widehat{\mathbb{B}}'_{U\rightarrow U})\in\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}}\times\mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}},\ \begin{pmatrix} b'^{(V\rightsquigarrow W)}_{1,1}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{1,1} & \cdots\cdots & b'^{(V\rightsquigarrow W)}_{1,\mathfrak{m}}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow W)}_{m_W,1}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{m_W,1} & \cdots\cdots & b'^{(V\rightsquigarrow W)}_{m_W,\mathfrak{m}}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{m_W,\mathfrak{m}} \\ b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W,1}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W,1} & & b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W,\mathfrak{m}}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W,\mathfrak{m}} \\ b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+1,1}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+1,1} & \cdots\cdots & b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+1,\mathfrak{m}}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,1}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,1} & & b'^{(V\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{m}}+i\ \widehat{b}'^{(W\rightsquigarrow W)}_{\mathcal{M}_W+\mathcal{L}_W,\mathfrak{m}} \end{pmatrix}\right)}$$

4. Description of Various Types of Cyber Attacks

4.1 Passive cyber-attacks conducted by APTs

A detailed mathematical description of a basic passive attack is given in **[6]**. There are though some potential differences between a basic passive cyber-attack (conducted by a non-persistent and non-sophisticated actor, i.e. hacktivist) and that conducted by an APT. In the following paragraphs we describe contextually these differences. The APT entity will be presented as $\boldsymbol{U_{APT}}$ in this section.

Let $\boldsymbol{U_{APT}, V} \in \boldsymbol{ob}\big(\boldsymbol{cy}(\boldsymbol{t})\big)$, whenever $\boldsymbol{t}$ is in an arbitrary subset $\mathbb{I} =]\boldsymbol{\sigma}, \boldsymbol{\tau}[\subset\subset [\mathbf{0}, \mathbf{1}]$. Let also

$$\boldsymbol{\delta_U}\colon [\mathbf{0}, \mathbf{1}] \to \mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\colon \boldsymbol{t} \mapsto \boldsymbol{\delta_W}(\boldsymbol{t}) = (\mathbb{z}_1, \mathbb{w}_1)(\boldsymbol{t}) \text{ and}$$

$$\boldsymbol{\gamma_V}\colon [\mathbf{0}, \mathbf{1}] \to \mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\colon \boldsymbol{t} \mapsto \boldsymbol{\gamma_V}(\boldsymbol{t}) = (\mathbb{z}_2, \mathbb{w}_2)(\boldsymbol{t})$$

be two supervisory perception curves of $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$ in the node system $(\boldsymbol{U_{APT}}, \boldsymbol{V})$.

A family of interactions

$$\boldsymbol{\mathcal{F}} = \big\{\boldsymbol{\mathcal{Z}} = \boldsymbol{\mathcal{Z}_{(Y,X)}}(\boldsymbol{t}) = \big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\big)(\boldsymbol{t}) \in \big(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\big)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I}\big\},$$

$\boldsymbol{X}, \boldsymbol{Y} \in \{\boldsymbol{U_{APT}}, \boldsymbol{V}\}$, with associated family of cyber-interplays [6]

$$\boldsymbol{\mathcal{D}_{\mathcal{F}}} = \Big\{\boldsymbol{\mathcal{G}} = \boldsymbol{\mathcal{G}^{(\mathcal{Z})}}\colon \mathbb{I} \to \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{X})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{Y})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{X})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{Y})}\colon$$

$$\boldsymbol{t} \mapsto \boldsymbol{\mathcal{G}}(\boldsymbol{t}) = \Big(\boldsymbol{\delta}_{\boldsymbol{Y}}^{(\mathcal{Z})}(\boldsymbol{t}), \boldsymbol{\gamma}_{\boldsymbol{X}}^{(\mathcal{Z})}(\boldsymbol{t}), \boldsymbol{\delta}_{\boldsymbol{Y}}^{(\mathcal{Z})}(\boldsymbol{t}+\Delta\boldsymbol{t}), \boldsymbol{\gamma}_{\boldsymbol{X}}^{(\mathcal{Z})}(\boldsymbol{t}+\Delta\boldsymbol{t})\Big)\colon \boldsymbol{t}+\Delta\boldsymbol{t} \in \mathbb{I}, \boldsymbol{\mathcal{Z}} \in \boldsymbol{\mathcal{F}}\Big\}$$

of the ordered cyber pair $(\boldsymbol{Y}, \boldsymbol{X})$ over the time $\boldsymbol{t} \in \mathbb{I}$**,** is called **coherent interactive family** in $\mathbb{I}$, if there is a homotopy

$$\boldsymbol{H}\colon \mathbb{I} \times [\mathbf{0}, \mathbf{1}] \to \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{X})} \times \mathbb{G}_{\boldsymbol{t}}^{(\boldsymbol{Y})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{X})} \times \mathbb{G}_{\boldsymbol{t}+\Delta\boldsymbol{t}}^{(\boldsymbol{Y})}$$

such that, for each cyber-interplay $\boldsymbol{\mathcal{G}} = \boldsymbol{\mathcal{G}}^{(\mathcal{Z})} \in \boldsymbol{\mathcal{D}}_{\mathcal{F}}$ there is a $\boldsymbol{p} \in [\mathbf{0}, \mathbf{1}]$ satisfying $\boldsymbol{H}(\boldsymbol{t}, \boldsymbol{p}) = \boldsymbol{\mathcal{G}}(\boldsymbol{t})$ at any moment time $\boldsymbol{t} \in \mathbb{I}$ on which the cyber-interplay $\boldsymbol{\mathcal{G}} = \boldsymbol{\mathcal{G}}^{(\mathcal{Z})}$ implements the interaction $\boldsymbol{\mathcal{Z}}$.

Proposition 4.1 In a passive attack $\boldsymbol{\mathcal{F}}$ defined in **[6]** from $\boldsymbol{U_{APT}}$ against $\boldsymbol{V}$, the number of resource parts in $\boldsymbol{U_{APT}}$ at a moment $\boldsymbol{t'} = \boldsymbol{t} + \Delta\boldsymbol{t}$ increased by at least $\boldsymbol{\lambda}$ new resource parts, say $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+2}\right)$,…, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda}\right)$, derived from the resource parts $\boldsymbol{fr}\left(\boldsymbol{res}^{(V)}_{\kappa_1}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}^{(V)}_{\kappa_2}\right)$,…,$\boldsymbol{fr}\left(\boldsymbol{res}^{(V)}_{\kappa_\lambda}\right)$ that existed in the node $\boldsymbol{V}$ the moment $\boldsymbol{t}$, in such a way that the following elementary properties hold:

i. If the relative valuations of $\boldsymbol{fr}\left(\boldsymbol{res}^{(U)}_{\mathcal{M}_V+\ell_V+1}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U)}_{\mathcal{M}_V+\ell_V+2}\right)$,…, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U)}_{\mathcal{M}_V+\ell_V+\lambda}\right)$ from the viewpoint of the (user(s) of) node $\boldsymbol{U_{APT}}$ at the moment $\boldsymbol{t}$ are $\left(\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_1,1}, \dots, \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_1,\mathfrak{n}}\right)$,…,$\left(\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\lambda,1}, \dots, \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\lambda,\mathfrak{n}}\right)$ respectively, with $\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\lambda} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{\ell_V}\}$, then the resulting valuation vectors $\left(\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1,1}, \dots, \widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1,\mathfrak{n}}\right)$,…,$\left(\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda,1}, \dots, \widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda,\mathfrak{n}}\right)$ of the **new** resource parts $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+2}\right)$,…, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda}\right)$ in $\boldsymbol{U}$, as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at a next moment $\boldsymbol{t'} = \boldsymbol{t} + \Delta\boldsymbol{t}$ are equal to $\left(\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_1,1}, \dots, \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_1,\mathfrak{n}}\right)$,…,$\left(\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\lambda,1}, \dots, \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\lambda,\mathfrak{n}}\right)$**:**

$$\left(\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\alpha,1}, \dots, \widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\alpha,\mathfrak{n}}\right) = \left(\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\alpha,1}, \dots, \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\mu_\alpha,\mathfrak{n}}\right), \forall\boldsymbol{\alpha} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{\lambda}\}.$$

ii. All resulting valuations and vulnerabilities of **new** resource parts $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1}\right)$,…, $\boldsymbol{fr}\left(\boldsymbol{res}^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda}\right)$ in $\boldsymbol{U_{APT}}$ from the viewpoint of the user(s) of $\boldsymbol{V}$ or any non-APT related node remain equal to **0:**

$$\forall\boldsymbol{j} \in \{\mathbf{1}, \mathbf{2}, \dots, \mathfrak{n}\}\ \boldsymbol{and}\ \forall\boldsymbol{\alpha} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{\lambda}\} \Longrightarrow \boldsymbol{a}'^{(V\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\alpha,j} = \mathbf{0},$$

$$\forall\boldsymbol{k} \in \{\mathbf{1}, \mathbf{2}, \dots, \mathfrak{m}\}\ \boldsymbol{and}\ \forall\boldsymbol{\alpha} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{\lambda}\} \Longrightarrow \boldsymbol{b}'^{(V\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\alpha,k} = \mathbf{0}.$$

iii. There is initially at least one resulting valuation $\boldsymbol{a'^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\lambda_\alpha,j}}$ of a part $\boldsymbol{fr\left(res^{(V)}_{\kappa_\alpha}\right)}$ in $\boldsymbol{V}$ from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ which decreases but for sure this number could be gradually increased: Initially

$$\exists \boldsymbol{j} \in \{\boldsymbol{1}, \boldsymbol{2}, \dots, \mathfrak{n}\}\ \boldsymbol{and}\ \exists \boldsymbol{\lambda_\alpha} \in \{\boldsymbol{\mathcal{M}_V + 1}, \dots, \boldsymbol{\mathcal{M}_V + \ell_V}\}: \boldsymbol{a'^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\lambda_\alpha,j}} < \boldsymbol{a^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\lambda_\alpha,j}};$$

similarly, there is initially at least one vulnerability $\boldsymbol{b'^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\rho_\alpha,k}}$ of part $\boldsymbol{fr\left(res^{(V)}_{\kappa_\alpha}\right)}$ in $\boldsymbol{V}$ from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ which increases but for sure this number could be gradually increased: Initially

$$\exists \boldsymbol{k} \in \{\boldsymbol{1}, \boldsymbol{2}, \dots, \mathfrak{m}\}\ \boldsymbol{and}\ \exists \boldsymbol{\rho_\alpha} \in \{\boldsymbol{\mathcal{M}_V + 1}, \dots, \boldsymbol{\mathcal{M}_V + \ell_V}\}: \boldsymbol{b'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\rho_\alpha,k}} > \boldsymbol{b^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\rho_\alpha,k}}.$$

iv. The valuations and vulnerabilities of each part $\boldsymbol{fr\left(res^{(V)}_{\kappa_\alpha}\right)}$ in $\boldsymbol{V}$ from the viewpoint of the user(s) of $\boldsymbol{V}$ remain unchanged until the first APT hunting results come up:

$$\forall \boldsymbol{j} \in \{\boldsymbol{1}, \boldsymbol{2}, \dots, \mathfrak{n}\}\ \boldsymbol{and}\ \forall \boldsymbol{\lambda_\alpha} \in \{\boldsymbol{\mathcal{M}_V + 1}, \dots, \boldsymbol{\mathcal{M}_V + \ell_V}\} \Longrightarrow \boldsymbol{\widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\lambda_\alpha,j}} = \boldsymbol{\widehat{a}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\lambda_\alpha,j}},$$

$$\forall \boldsymbol{k} \in \{\boldsymbol{1}, \boldsymbol{2}, \dots, \mathfrak{m}\}\ \boldsymbol{and}\ \forall \boldsymbol{\mu_\alpha} \in \{\boldsymbol{\mathcal{M}_V + 1}, \dots, \boldsymbol{\mathcal{M}_V + \ell_V}\} \Longrightarrow \boldsymbol{\widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V+\mu_\alpha,k}} = \boldsymbol{\widehat{b}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V+\mu_\alpha,k}}.$$ ■

Proposition 4.2 In a passive attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U_{APT}}$ against $\boldsymbol{V}$, the number of resource parts in $\boldsymbol{U_{APT}}$ at a moment $\boldsymbol{t' = t + \Delta t}$ has increased by at least $\boldsymbol{\lambda}$ new resource parts, say $\boldsymbol{fr\left(res^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+1}\right)}$, $\boldsymbol{fr\left(res^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+2}\right)}$,…, $\boldsymbol{fr\left(res^{(U_{APT})}_{\mathcal{M}_{U_{APT}}+\ell_{U_{APT}}+\lambda}\right)}$, derived from the resource parts $\boldsymbol{fr\left(res^{(V)}_{\kappa_1}\right)}$, $\boldsymbol{fr\left(res^{(V)}_{\kappa_2}\right)}$,…,$\boldsymbol{fr\left(res^{(V)}_{\kappa_\lambda}\right)}$ that existed in the node $\boldsymbol{V}$ the moment $\boldsymbol{t}$, in such a way that the following elementary properties hold.

i. The (Euclidean) norm $\left\|\boldsymbol{\widehat{a}'^{(U_{APT}\rightsquigarrow U_{APT})}}\right\| := \left(\sum_{j=1}^{\mathfrak{n}} \sum_{\nu=1}^{\boldsymbol{\ell_{U_{APT}}+\lambda}} \left|\boldsymbol{\widehat{a}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\nu,j}}\right|^2\right)^{1/2}$ of the resulting overall valuation in the variant node $\boldsymbol{U_{APT}'}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **much greater** than the (Euclidean) norms

$$\left\|\boldsymbol{\widehat{a}^{(U_{APT}\rightsquigarrow U_{APT})}}\right\| := \left(\sum_{j=1}^{\mathfrak{n}} \sum_{\nu=1}^{\boldsymbol{\ell_U}} \left|\boldsymbol{\widehat{a}^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\nu,j}}\right|^2\right)^{1/2} \text{ and}$$

$$\left\|\boldsymbol{a^{(U_{APT}\rightsquigarrow V)}}\right\| := \left(\sum_{j=1}^{\mathfrak{n}} \sum_{\nu=1}^{\boldsymbol{\ell_V}} \left|\boldsymbol{a^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\nu,j}}\right|^2\right)^{1/2}$$

of the initial overall valuations in the nodes $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the users of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{\widehat{a}'^{(U_{APT}\rightsquigarrow U_{APT})}}\right\| \gg max\left\{\left\|\boldsymbol{\widehat{a}^{(U_{APT}\rightsquigarrow U_{APT})}}\right\|, \left\|\boldsymbol{a^{(U_{APT}\rightsquigarrow V)}}\right\|\right\}.$$

ii. The norm $\left\|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{n}}\sum_{\nu=1}^{\ell_V}\left|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\nu,j}\right|^2\right)^{1/2}$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **much less** than the norm $\left\|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{n}}\sum_{\nu=1}^{\ell_V}\left|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\nu,j}\right|^2\right)^{1/2}$ of the initial overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the users of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}\right\| \ll \left\|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}\right\|.$$

iii. The norm $\left\|\widehat{\boldsymbol{b}}'^{(U_{APT}\rightsquigarrow U_{APT})}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\ell_{U_{APT}}+\nu}\left|\widehat{\boldsymbol{b}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}U}+\lambda,j}\right|^2\right)^{1/2}$ of the resulting overall vulnerability in the variant node $\boldsymbol{U_{APT}}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **less** than the norms

$$\left\|\widehat{\boldsymbol{b}}^{(U_{APT}\rightsquigarrow U_{APT})}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\nu=1}^{\ell_W}\left|\widehat{\boldsymbol{b}}^{(U_{APT}\rightsquigarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\nu,j}\right|^2\right)^{1/2} \text{ and}$$

$$\left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\nu=1}^{\ell_V}\left|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\nu,j}\right|^2\right)^{1/2}$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the users of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(U_{APT}\rightsquigarrow U_{APT})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(U_{APT}\rightsquigarrow U_{APT})}\right\|, \left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|\right\}.$$

iv. The norm $\left\|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\nu=1}^{\ell_V}\left|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_V+\nu,j}\right|^2\right)^{1/2}$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the users of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **much greater** than the norm $\left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\nu=1}^{\ell_V}\left|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}_{\mathcal{M}_{U_{APT}}+\nu,j}\right|^2\right)^{1/2}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}\right\| \gg \left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|.\blacksquare$$

4.2 Active cyber-attacks conducted by APTs

An attack is active if it is an attack with data transmission to all parties thereby acting as a liaison enabling severe compromise. The purpose is to alter system resources

or affect their operation. So, in an active attack, an intruder attempts to alter data on the target system or data "en route" for the target system. A detailed mathematical description of a basic active attack is given in **[6]**. There are though some potential differences between a basic active cyber-attack (conducted by a non- persistent and non-sophisticated actor, i.e. hacktivist) and that conducted by an APT. In the following paragraphs we describe contextually these differences. The APT entity will be presented as $\boldsymbol{U_{APT}}$

Let $\boldsymbol{U_{APT}}, \boldsymbol{V} \in \boldsymbol{ob}\big(\boldsymbol{cy}(\boldsymbol{t})\big)$, whenever $\boldsymbol{t}$ is in an arbitrary interval $\mathbb{I} =]\boldsymbol{\sigma}, \boldsymbol{\tau}[\subset\subset [\mathbf{0}, \mathbf{1}]$. Let also

$$\boldsymbol{\delta_U}\colon [\mathbf{0}, \mathbf{1}] \to \mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\colon \boldsymbol{t} \mapsto \boldsymbol{\delta_U}(\boldsymbol{t}) = (\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}})(\boldsymbol{t}) \text{ and}$$

$$\boldsymbol{\gamma_V}\colon [\mathbf{0}, \mathbf{1}] \to \mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\colon \boldsymbol{t} \mapsto \boldsymbol{\gamma_V}(\boldsymbol{t}) = (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})(\boldsymbol{t})$$

be two supervisory perception curves of $\boldsymbol{V}$ and $\boldsymbol{U_{APT}}$ in the node system $(\boldsymbol{V}, \boldsymbol{U_{APT}})$.

Proposition 4.3 In an active attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U_{APT}}$ against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})$ −device parts $\boldsymbol{fr}\Big(\boldsymbol{dev}^{(V)}_{\boldsymbol{\mu_1}}\Big)$,…,$\boldsymbol{fr}\Big(\boldsymbol{dev}^{(V)}_{\boldsymbol{\mu_\nu}}\Big)$ of $\boldsymbol{V}$ and the $(\boldsymbol{\kappa_1}, \dots, \boldsymbol{\kappa_\lambda})-$ resource parts $\boldsymbol{fr}\Big(\boldsymbol{res}^{(V)}_{\boldsymbol{\kappa_1}}\Big)$,…,$\boldsymbol{fr}\Big(\boldsymbol{res}^{(V)}_{\boldsymbol{\kappa_\lambda}}\Big)$ of $\boldsymbol{V}$, the following elementary properties hold.

i. All **new** resource valuations of the offensive node $\boldsymbol{U_{APT}}$ are derived from the set of all initial resource valuations of $\boldsymbol{V}$, i.e., for any $\boldsymbol{j} \in \big\{\boldsymbol{\mathcal{M}}_{\boldsymbol{U_{APT}}} + \boldsymbol{\ell}_{\boldsymbol{U_{APT}}} + \mathbf{1}, \dots, \boldsymbol{\mathcal{M}}_{\boldsymbol{U_{APT}}} + \boldsymbol{\ell}_{\boldsymbol{U_{APT}}} + \boldsymbol{N}\big\}$ and any $\boldsymbol{k} \in \{\mathbf{1}, \mathbf{2}, \dots, \mathfrak{n}\}$, the new valuations

$$\boldsymbol{a'}^{(\boldsymbol{V}\nrightarrow\boldsymbol{U_{APT}})}_{\boldsymbol{j,k}} + \boldsymbol{i\widehat{a}'}^{(\boldsymbol{U_{APT}}\nrightarrow\boldsymbol{U_{APT}})}_{\boldsymbol{j,k}}$$

are obtained as functions of the initial valuations

$$\boldsymbol{a}^{(\boldsymbol{U_{APT}}\nrightarrow\boldsymbol{V})}_{\boldsymbol{p,l}} + \boldsymbol{i\widehat{a}}^{(\boldsymbol{V}\nrightarrow\boldsymbol{V})}_{\boldsymbol{p,l}}, \boldsymbol{p} \in \{\mathbf{1}, \mathbf{2}, \dots, \boldsymbol{m_V}, \boldsymbol{\mathcal{M}_V} + \mathbf{1}, \dots, \boldsymbol{\mathcal{M}_V} + \boldsymbol{\ell_V}\}, \boldsymbol{l} \in \{\mathbf{1}, \mathbf{2}, \dots, \mathfrak{n}\}.$$

ii. Similarly, all **new** resource vulnerabilities of the offensive node $\boldsymbol{U_{APT}}$ are derived from the set of all initial resource vulnerabilities of $\boldsymbol{V}$, i.e., for any $\boldsymbol{j} \in \big\{\boldsymbol{\mathcal{M}}_{\boldsymbol{U_{APT}}} + \boldsymbol{\ell}_{\boldsymbol{U_{APT}}} + \mathbf{1}, \dots, \boldsymbol{\mathcal{M}}_{\boldsymbol{U_{APT}}} + \boldsymbol{\ell}_{\boldsymbol{U_{APT}}} + \boldsymbol{N}\big\}$ and any $\boldsymbol{k} \in \{\mathbf{1}, \mathbf{2}, \dots, \mathfrak{n}\}$, the new vulnerabilities

$$\boldsymbol{b'}^{(\boldsymbol{V}\nrightarrow\boldsymbol{U_{APT}})}_{\boldsymbol{j,k}} + \boldsymbol{i\widehat{b}'}^{(\boldsymbol{U_{APT}}\nrightarrow\boldsymbol{U_{APT}})}_{\boldsymbol{j,k}}$$

are obtained as functions of the initial vulnerabilities

$$\boldsymbol{b}_{p,l}^{(U_{APT}\rightsquigarrow V)}+\boldsymbol{i}\widehat{\boldsymbol{b}}_{p,l}^{(V\rightsquigarrow V)},\boldsymbol{p}\in\{\mathbf{1},\mathbf{2},\dots,\boldsymbol{m}_{V},\boldsymbol{\mathcal{M}}_{V}+\mathbf{1},\dots,\boldsymbol{\mathcal{M}}_{V}+\boldsymbol{\ell}_{V}\},\boldsymbol{k}\in\{\mathbf{1},\mathbf{2},\dots,\mathfrak{m}\}.$$

iii. Finally, from the viewpoint of the (user(s) of) node $\boldsymbol{V}$, all valuations, if possible, of $\boldsymbol{U_{APT}}$ remain unchanged, i.e., if $\boldsymbol{j}\in\{\mathbf{1},\mathbf{2},\dots,\boldsymbol{m}_{U_{APT}},\boldsymbol{\mathcal{M}}_{U_{APT}}+\mathbf{1},\dots,\boldsymbol{\mathcal{M}}_{U_{APT}}+\boldsymbol{\ell}_{U_{APT}}\}$, then $\boldsymbol{a}_{j,k}^{(V\rightsquigarrow U_{APT})}=\boldsymbol{a}'^{(V\rightsquigarrow U_{APT})}_{j,k}$ for any $\boldsymbol{k}\in\{\mathbf{1},\mathbf{2},\dots,\mathfrak{n}\}$ and $\boldsymbol{b}_{j,k}^{(V\rightsquigarrow U_{APT})}=\boldsymbol{b}'^{(V\rightsquigarrow U_{APT})}_{j,k}$ for any $\boldsymbol{k}\in\{\mathbf{1},\mathbf{2},\dots,\mathfrak{m}\}$. ■

Proposition 4.4 In an active attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U_{APT}}$ against the $(\boldsymbol{\mu_1},\dots,\boldsymbol{\mu_\nu})$ −device parts $\boldsymbol{fr}\left(\boldsymbol{dev}_{\mu_1}^{(V)}\right),\dots,\boldsymbol{fr}\left(\boldsymbol{dev}_{\mu_\nu}^{(V)}\right)$ of $\boldsymbol{V}$ and the $(\boldsymbol{\kappa_1},\dots,\boldsymbol{\kappa_\lambda})-$ resource parts $\boldsymbol{fr}\left(\boldsymbol{res}_{\kappa_1}^{(V)}\right),\dots,\boldsymbol{fr}\left(\boldsymbol{res}_{\kappa_\lambda}^{(V)}\right)$ of $\boldsymbol{V}$, the following elementary properties hold.

i. The (Euclidean) norm $\left\|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{n}}\sum_{\lambda=1}^{\boldsymbol{\ell}_V}\left|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}_{\boldsymbol{\mathcal{M}}_V+\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}\right)^{\mathbf{1/2}}$ of the resulting overall valuation in node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t}'$ is **much less** than the (Euclidean) norm $\left\|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{n}}\sum_{\lambda=1}^{\boldsymbol{\ell}_V}\left|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}_{\boldsymbol{\mathcal{M}}_V+\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}\right)^{\mathbf{1/2}}$ of the initial overall valuation in $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{a}'^{(U_{APT}\rightsquigarrow V)}\right\|\ll\left\|\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}\right\|.$$

ii. The (Euclidean) norm $\left\|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\boldsymbol{\ell}_V}\left|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}_{\boldsymbol{\mathcal{M}}_V+\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}\right)^{\mathbf{1/2}}$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t}'$ is **much greater** than the (Euclidean) norm $\left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|:=\left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\boldsymbol{\ell}_V}\left|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}_{\boldsymbol{\mathcal{M}}_V+\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}\right)^{\mathbf{1/2}}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{b}'^{(U_{APT}\rightsquigarrow V)}\right\|\gg\left\|\boldsymbol{b}^{(U_{APT}\rightsquigarrow V)}\right\|.$$

iii. The (Euclidean) norm

$$\left\|\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}\right\|:=\left(\sum_{j=1}^{\mathfrak{n}}\left\{\sum_{\lambda=1}^{\boldsymbol{m}_{U_{APT}}}\left|\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}+\sum_{\lambda=1}^{\boldsymbol{\ell}_{U_{APT}}+\boldsymbol{N}}\left|\widehat{\boldsymbol{a}}'^{(U_{APT}\rightsquigarrow U_{APT})}_{\boldsymbol{\mathcal{M}}_{U_{APT}}+\boldsymbol{\lambda},\boldsymbol{j}}\right|^{\mathbf{2}}\right\}\right)^{\mathbf{1/2}}$$

of the resulting overall valuation in the variant node $\boldsymbol{U_{APT}}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **much greater** than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{a}}^{(U_{APT}\twoheadrightarrow U_{APT})}\right\| := \left(\sum_{j=1}^{\mathfrak{n}}\left\{\sum_{\lambda=1}^{m_{U_{APT}}}\left|\widehat{a}_{\lambda,j}^{(U_{APT}\twoheadrightarrow U_{APT})}\right|^2+\sum_{\lambda=1}^{\ell_W}\left|\widehat{a}_{\mathcal{M}_{U_{APT}}+\lambda,j}^{(U_{APT}\twoheadrightarrow U_{APT})}\right|^2\right\}\right)^{1/2}$$

and

$$\left\|\boldsymbol{a}^{(U_{APT}\twoheadrightarrow V)}\right\| := \left(\sum_{j=1}^{\mathfrak{n}}\left\{\sum_{\lambda=1}^{m_V}\left|a_{\lambda,j}^{(U_{APT}\twoheadrightarrow V)}\right|^2+\sum_{\lambda=1}^{\ell_V}\left|a_{\mathcal{M}_V+\lambda,j}^{(U_{APT}\twoheadrightarrow V)}\right|^2\right\}\right)^{1/2}$$

of the initial overall valuations in the nodes $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{a}}'^{(U_{APT}\twoheadrightarrow U_{APT})}\right\| \gg \boldsymbol{max}\left\{\left\|\widehat{\boldsymbol{a}}^{(U_{APT}\twoheadrightarrow U_{APT})}\right\|, \left\|\boldsymbol{a}^{(U_{APT}\twoheadrightarrow V)}\right\|\right\}.$$

iv. The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}'^{(U_{APT}\twoheadrightarrow U_{APT})}\right\| := \left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\ell_{U_{APT}}+N}\left|\widehat{b}'^{(U_{APT}\twoheadrightarrow U_{APT})}_{\mathcal{M}_U+\lambda,j}\right|^2\right)^{1/2}$

of the resulting overall vulnerability in the variant node $\boldsymbol{U_{APT}}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the next moment $\boldsymbol{t'}$ is **less** than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(U_{APT}\twoheadrightarrow U_{APT})}\right\| := \left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\ell_{U_{APT}}}\left|\widehat{b}^{(U_{APT}\twoheadrightarrow U_{APT})}_{\mathcal{M}_{U_{APT}}+\lambda,j}\right|^2\right)^{1/2} \text{ and}$$

$$\left\|\boldsymbol{b}^{(U_{APT}\twoheadrightarrow V)}\right\| := \left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\ell_V}\left|b^{(U_{APT}\twoheadrightarrow V)}_{\mathcal{M}_{U_{APT}}+\lambda,j}\right|^2\right)^{1/2}$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U_{APT}}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(U_{APT}\twoheadrightarrow U_{APT})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(U_{APT}\twoheadrightarrow U_{APT})}\right\|, \left\|\boldsymbol{b}^{(U_{APT}\twoheadrightarrow V)}\right\|\right\}. \blacksquare$$

5. Mathematical Description of Indications of Compromise (IOCs) related to APTs

So, having examined the more general cases of a passive and active attacks, we will try to focus on some IOCs related to APT actors' activities.

In order to go further and get the full description of these IOCs, it would be wise to mathematically orient and define some further concepts. The sophistication of development of any cyber-attack is a critical issue and can be described as follows.

5.1 Sophistication of APT Cyber Attacks

The term "sophistication" of a cyber-attack is often used inconsistently or incorrectly by the cyber community, let alone in the cases where a persistent, advanced and complex actor (as APT) is involved. Generally, most of the times the term "sophistication" is used inadvertently or deliberately. The term, even though it is highly important and critical, loses its value when overused, and should instead be employed to differentiate exceptional attacks or attackers from the norm (as an APT may be).

The "sophistication" of a cyber-attack concept is a puzzle of definitions that form the big picture. To enter the structural operational status of such a **"sophisticated" attack puzzle**, we assume *the derivatives*

$$\boldsymbol{\varphi}^{(U_{APT}\rightsquigarrow V)}(\boldsymbol{t}) := \frac{\partial\{a^{(U_{APT}\rightsquigarrow V)}\}}{\partial \boldsymbol{t}}(\boldsymbol{t}) = \frac{\partial\{\left(a_{\mathbf{1}}^{(U_{APT}\rightsquigarrow V)},\dots a_{m_V}^{(U_{APT}\rightsquigarrow V)},a_{m_V+1}^{(U_{APT}\rightsquigarrow V)},\dots,a_{\mathcal{M}_V}^{(U_{APT}\rightsquigarrow V)},a_{\mathcal{M}_V+1}^{(U_{APT}\rightsquigarrow V)},\dots,a_{\mathcal{M}_V+\ell_V+1}^{(U_{APT}\rightsquigarrow V)},a_{\mathcal{M}_V+\ell_V+1}^{(U_{APT}\rightsquigarrow V)},\dots,a_{\mathcal{M}_V+\mathcal{L}_V}^{(U_{APT}\rightsquigarrow V)}\right)^{T}\}}{\partial \boldsymbol{t}}(\boldsymbol{t})$$

and

$$\widehat{\boldsymbol{\varphi}}^{(V\rightsquigarrow V)}(\boldsymbol{t}) := \frac{\partial\{\widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}[\boldsymbol{x_1},\boldsymbol{x_2},\boldsymbol{x_3},\boldsymbol{t}\,]\}}{\partial \boldsymbol{t}}(\boldsymbol{t}) = \frac{\partial\{\left(\widehat{a}_{\mathbf{1}}^{(V\rightsquigarrow V)},\dots \widehat{a}_{m_V}^{(V\rightsquigarrow V)},\widehat{a}_{m_V+1}^{(V\rightsquigarrow V)},\dots,\widehat{a}_{\mathcal{M}_V}^{(V\rightsquigarrow V)},\widehat{a}_{\mathcal{M}_V+1}^{(V\rightsquigarrow V)},\dots,\widehat{a}_{\mathcal{M}_V+\ell_V+1}^{(V\rightsquigarrow V)},\widehat{a}_{\mathcal{M}_V+\ell_V+1}^{(V\rightsquigarrow V)},\dots,\widehat{a}_{\mathcal{M}_V+\mathcal{L}_V}^{(V\rightsquigarrow V)}\right)^{T}\}}{\partial \boldsymbol{t}}(\boldsymbol{t})$$

exist in a time interval $\mathbb{I} =]\boldsymbol{\alpha},\boldsymbol{\beta}[$ *in the sense of distributions*. In such a case, we say that the relative effectiveness states $\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)} = \boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}[\boldsymbol{x_1},\boldsymbol{x_2},\boldsymbol{x_3},\boldsymbol{t}\,] \in \mathbb{R}^{\boldsymbol{\kappa}}$ and $\widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)} = \widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}[\boldsymbol{x_1},\boldsymbol{x_2},\boldsymbol{x_3},\boldsymbol{t}\,] \in \mathbb{R}^{\boldsymbol{\kappa}}$ are two **smooth node valuations** and the distributional derivatives $\boldsymbol{\varphi}^{(U_{APT}\rightsquigarrow V)}(\boldsymbol{t})$ and $\widehat{\boldsymbol{\varphi}}^{(V\rightsquigarrow V)}(\boldsymbol{t})$ are the **rate changes/slopes of the valuations** $\boldsymbol{a}^{(U_{APT}\rightsquigarrow V)}$ and $\widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}$ respectively, at a point $(\boldsymbol{x_1},\boldsymbol{x_2},\boldsymbol{x_3}\,)$ of a part $\boldsymbol{E}$ into the node $\boldsymbol{V}$ from the viewpoint of the (user(s) of) node $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$, respectively, over the time interval $\mathbb{I}$. Here, as usually, $\boldsymbol{\kappa} := \boldsymbol{\mathcal{M}_V} + \boldsymbol{\mathcal{L}_V}$.

For $\boldsymbol{\Phi} = \boldsymbol{\varphi},\widehat{\boldsymbol{\varphi}}$ and $\boldsymbol{X},\boldsymbol{Y} \in \{\boldsymbol{U_{APT}},\boldsymbol{V}\}$, it is obvious that

1. If $\boldsymbol{\Phi}^{(X\rightsquigarrow Y)}(\boldsymbol{t}) > \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$**,** then we are situated definitely in the area $[\boldsymbol{\mathcal{A}}_{\boldsymbol{X}}^{+}(\boldsymbol{Y})](\mathbb{I})$ of correlated growth for the total valuation of the node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$ ([5]).
2. If $\boldsymbol{\Phi}^{(X\rightsquigarrow Y)}(\boldsymbol{t}) < \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$**,** then we are situated definitely in the area $[\boldsymbol{\mathcal{A}}_{\boldsymbol{X}}^{-}(\boldsymbol{Y})](\mathbb{I})$ of correlated reduction for the total valuation of the node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$ ([5]).

3. If $\boldsymbol{\Phi}^{(X \rightsquigarrow Y)}(\boldsymbol{t}) = \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$, there is no correlated growth or reduction for the total valuation of the node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$, due to a multitude of potential reasons.

By analogy, suppose *the derivatives*

$$\boldsymbol{\psi}^{(U_{APT} \rightsquigarrow V)}(\boldsymbol{t}) := \frac{\boldsymbol{\partial}\{\boldsymbol{b}^{(U_{APT} \rightsquigarrow V)}[\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}\,]\}}{\boldsymbol{\partial t}}(\boldsymbol{t}) =$$

$$\frac{\boldsymbol{\partial}\{\left(\boldsymbol{b}_{\mathbf{1}}^{(U_{APT} \rightsquigarrow V)}, \ldots, \boldsymbol{b}_{\boldsymbol{m_V}}^{(U_{APT} \rightsquigarrow V)}, \boldsymbol{b}_{\boldsymbol{m_V+1}}^{(U_{APT} \rightsquigarrow V)}, \ldots, \boldsymbol{b}_{\boldsymbol{\mathcal{M}_V}}^{(U_{APT} \rightsquigarrow V)}, \boldsymbol{b}_{\boldsymbol{\mathcal{M}_V+1}}^{(U_{APT} \rightsquigarrow V)}, \ldots, \boldsymbol{b}_{\boldsymbol{\mathcal{M}_V+\ell_V+1}}^{(U_{APT} \rightsquigarrow V)}, \boldsymbol{b}_{\boldsymbol{\mathcal{M}_V+\ell_V+1}}^{(U_{APT} \rightsquigarrow V)}, \ldots, \boldsymbol{b}_{\boldsymbol{\mathcal{M}_V+\mathcal{L}_V}}^{(U_{APT} \rightsquigarrow V)}\right)^{\boldsymbol{T}}\}}{\boldsymbol{\partial t}}(\boldsymbol{t})$$

and

$$\widehat{\boldsymbol{\psi}}^{(V \rightsquigarrow V)}(\boldsymbol{t}) := \frac{\boldsymbol{\partial}\{\widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}[\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}\,]\}}{\boldsymbol{\partial t}}(\boldsymbol{t}) =$$

$$\frac{\boldsymbol{\partial}\{\left(\widehat{\boldsymbol{b}}_{\mathbf{1}}^{(V \rightsquigarrow V)}, \ldots, \widehat{\boldsymbol{b}}_{\boldsymbol{m_V}}^{(V \rightsquigarrow V)}, \widehat{\boldsymbol{b}}_{\boldsymbol{m_V+1}}^{(V \rightsquigarrow V)}, \ldots, \widehat{\boldsymbol{b}}_{\boldsymbol{\mathcal{M}_V}}^{(V \rightsquigarrow V)}, \widehat{\boldsymbol{b}}_{\boldsymbol{\mathcal{M}_V+1}}^{(V \rightsquigarrow V)}, \ldots, \widehat{\boldsymbol{b}}_{\boldsymbol{\mathcal{M}_V+\ell_V+1}}^{(V \rightsquigarrow V)}, \widehat{\boldsymbol{b}}_{\boldsymbol{\mathcal{M}_V+\ell_V+1}}^{(V \rightsquigarrow V)}, \ldots, \widehat{\boldsymbol{b}}_{\boldsymbol{\mathcal{M}_V+\mathcal{L}_V}}^{(V \rightsquigarrow V)}\right)^{\boldsymbol{T}}\}}{\boldsymbol{\partial t}}(\boldsymbol{t})$$

exist in a time interval $\mathbb{I} =]\boldsymbol{\alpha}, \boldsymbol{\beta}[$ *in the sense of distributions*. In such a case, we say that the relative effectiveness states $\boldsymbol{b}^{(U_{APT} \rightsquigarrow V)} = \boldsymbol{b}^{(U_{APT} \rightsquigarrow V)}[\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}\,] \in \mathbb{R}^{\boldsymbol{k}}$ and $\widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)} = \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}[\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}, \boldsymbol{t}\,] \in \mathbb{R}^{\boldsymbol{k}}$ are two **smooth node vulnerabilities** and the distributional derivatives $\boldsymbol{\psi}^{(U_{APT} \rightsquigarrow V)}(\boldsymbol{t})$ and $\widehat{\boldsymbol{\psi}}^{(V \rightsquigarrow V)}(\boldsymbol{t})$ are the **rate changes/slopes of the vulnerabilities** $\boldsymbol{b}^{(U_{APT} \rightsquigarrow V)}$ and $\widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}$ respectively, at a point $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{x_3}\,)$ of a part $\boldsymbol{E}$ into the node $\boldsymbol{V}$ from the viewpoint of the (user(s) of) node $\boldsymbol{U_{APT}}$ and $\boldsymbol{V}$, respectively, over the time interval $\mathbb{I}$.

As above, for $\boldsymbol{\Psi} = \boldsymbol{\psi}, \widehat{\boldsymbol{\psi}}$ and $\boldsymbol{X}, \boldsymbol{Y} \in \{\boldsymbol{U_{APT}}, \boldsymbol{V}\}$, it is obvious that:

1. If $\boldsymbol{\Psi}^{(X \rightsquigarrow Y)}(\boldsymbol{t}) > \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$**,** then we are situated definitely in the area $[\boldsymbol{\mathcal{B}}_{\boldsymbol{X}}^{+}(\boldsymbol{Y})](\mathbb{I})$ of correlated growth for the total vulnerability of the node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$ ([5]).
2. If $\boldsymbol{\Psi}^{(X \rightsquigarrow Y)}(\boldsymbol{t}) < \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$**,** then we are situated definitely in the area $[\boldsymbol{\mathcal{B}}_{\boldsymbol{X}}^{-}(\boldsymbol{Y})](\mathbb{I})$ of correlated reduction for the total vulnerability of the node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$ ([5]).
3. If $\boldsymbol{\Psi}^{(X \rightsquigarrow Y)}(\boldsymbol{t}) = \mathbf{0}$ whenever $\boldsymbol{t} \in \mathbb{I}$, there is no correlated growth or reduction of the total vulnerability for node $\boldsymbol{Y}$ as evaluated subjectively from the user(s) of $\boldsymbol{X}$ over the time set $\mathbb{I}$, due to a multitude of potential reasons.

Remark 5.1 Having defined the rate change of valuations and vulnerabilities we can proceed to orientation of sophistication in cyber-attacks, definition which will support our further posture in this paper. So, if we have one or combination of the following

states that declare a slow infection (constituents' degradation) we assume that there should be a **suspicion of sophistication** $\widehat{\boldsymbol{\varphi}}^{(V\twoheadrightarrow V)} \cong \mathbf{0}^{-}$ and $\widehat{\boldsymbol{\psi}}^{(V\twoheadrightarrow V)} \cong \mathbf{0}^{+}$. ■

5.2 APT Hunting Scenario 1

The APT actor $\boldsymbol{Z_{APT}}$ secretly relays and possibly alters the communication between two parties/nodes who believe they are directly communicating with each other, belongs to active cyber-attacks.

In this scenario the **node $\boldsymbol{Z_{APT}}$,** that is the APT actor, cyber-interacts between nodes $\boldsymbol{U}$ and $\boldsymbol{V}$. Actually in this "active" intersection attack, instead of this "normal" interaction we experience an active attack from node $\boldsymbol{Z_{APT}}$ to either or/and both of other nodes **using some resources of the other interacted node**. In such a case, a family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \Big\{\boldsymbol{Z_{APT}} = \boldsymbol{Z_{APT}}_{(Y,X)}(\boldsymbol{t}) = \big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}), (\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\big)(\boldsymbol{t}) \in \big(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathcal{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathcal{k}}}\big)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I}\Big\},$$

lying in the partial danger sector $\mathcal{E} = \mathcal{E}_{\boldsymbol{Z_{APT}}\to\boldsymbol{V}}$ to the node $\boldsymbol{V}$ from the node $\boldsymbol{Z_{APT}}$ during the entire time set $\mathbb{I}$, is a **germ of (partial) active attack against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})$ − device parts $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_1}}^{(V)}\right)$, $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_2}}^{(V)}\right)$,..., $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_\nu}}^{(V)}\right)$ of $\boldsymbol{V}$ and the $(\boldsymbol{\kappa_1}, \dots, \boldsymbol{\kappa_\lambda})$ − resource parts $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_1}}^{(V)}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_2}}^{(V)}\right)$,..., $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_\lambda}}^{(V)}\right)$ of $\boldsymbol{V}$**, during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) \in \big(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathcal{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathcal{k}}}\big)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{Z_{APT}}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{Z_{APT}}$ and $\boldsymbol{V}$ has the form

$$\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) =$$

$$\left(\left(\left(\begin{array}{ccc}
\boldsymbol{a}_{1,1}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,1}^{(V\twoheadrightarrow V)} & \cdots & \boldsymbol{a}_{1,\mathfrak{n}}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,\mathfrak{n}}^{(V\twoheadrightarrow V)} \\
\cdots \quad \cdots & \cdots & \cdots \quad \cdots \\
\boldsymbol{a}_{\boldsymbol{m_V},1}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{m_V},1}^{(V\twoheadrightarrow V)} & & \boldsymbol{a}_{\boldsymbol{m_V},\mathfrak{n}}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{m_V},\mathfrak{n}}^{(V\twoheadrightarrow V)} \\
\mathbf{0} \quad \cdots & \cdots & \mathbf{0} \quad \cdots \\
\mathbf{0} & \cdots & \mathbf{0} \\
\boldsymbol{a}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},1}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},1}^{(V\twoheadrightarrow V)} & \cdots & \boldsymbol{a}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{n}}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{n}}^{(V\twoheadrightarrow V)} \\
\cdots \quad \cdots & & \cdots \quad \cdots \\
\boldsymbol{a}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},1}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},1}^{(V\twoheadrightarrow V)} & \cdots & \boldsymbol{a}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{n}}^{(Z_{APT}\twoheadrightarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{n}}^{(V\twoheadrightarrow V)} \\
\mathbf{0} \quad \cdots & \cdots & \mathbf{0} \quad \cdots \\
\mathbf{0} & \cdots & \mathbf{0}
\end{array}\right)\right)\right),$$

$$\begin{pmatrix} \boldsymbol{b}_{1,1}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(V \rightsquigarrow V)} & \cdots & \boldsymbol{b}_{1,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{m}}^{(V \rightsquigarrow V)} \\ \cdots \\ \boldsymbol{b}_{m_V,1}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_V,1}^{(V \rightsquigarrow V)} & \cdots & \boldsymbol{b}_{m_V,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_V,\mathfrak{m}}^{(V \rightsquigarrow V)} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{b}_{\mathcal{M}_V+1,1}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_V+1,1}^{(V \rightsquigarrow V)} & \cdots & \boldsymbol{b}_{\mathcal{M}_V+1,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V \rightsquigarrow V)} \\ \cdots \\ \boldsymbol{b}_{\mathcal{M}_V+\ell_V,1}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_V+\ell_V,1}^{(V \rightsquigarrow V)} & \cdots & \boldsymbol{b}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow V)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(V \rightsquigarrow V)} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{pmatrix},$$

$$\begin{pmatrix} \begin{pmatrix} \boldsymbol{a}_{1,1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{a}_{1,\mathfrak{n}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,\mathfrak{n}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \cdots \\ \boldsymbol{a}_{m_{Z_{APT}},1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_{Z_{APT}},1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{a}_{m_{Z_{APT}},\mathfrak{n}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_{Z_{APT}},\mathfrak{n}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{a}_{\mathcal{M}_{Z_{APT}}+1,1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_{Z_{APT}}+1,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{a}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{n}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{n}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \cdots \\ \boldsymbol{a}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}}z,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{a}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{n}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{n}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{pmatrix} \end{pmatrix},$$

$$\begin{pmatrix} \begin{pmatrix} \begin{pmatrix} \boldsymbol{b}_{1,1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{1,\mathfrak{m}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \cdots \\ \boldsymbol{b}_{m_Z,1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_{Z_{APT}},1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{m_{Z_{APT}},\mathfrak{m}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_{Z_{APT}},\mathfrak{m}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+1,1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+1,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{m}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{m}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \cdots \\ \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},1}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}}z,1}^{(Z_{APT} \rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{m}}^{(V \rightsquigarrow Z_{APT})} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{m}}^{(Z_{APT} \rightsquigarrow Z_{APT})} \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{pmatrix} \end{pmatrix} \end{pmatrix}$$

and is depicted, at a next moment $\boldsymbol{t'} = \boldsymbol{t} + \Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\boldsymbol{1}}', \mathbb{w}_{\boldsymbol{1}}'), (\mathbb{z}_{\boldsymbol{2}}', \mathbb{w}_{\boldsymbol{2}}')\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\right)^{\boldsymbol{2}}$ of supervisory resource perceptions of $\boldsymbol{Z_{APT}} = \boldsymbol{Z}$ and $\boldsymbol{V}$ having the form

$\left((\mathbb{z}_{\boldsymbol{1}}', \mathbb{w}_{\boldsymbol{1}}'), (\mathbb{z}_{\boldsymbol{2}}', \mathbb{w}_{\boldsymbol{2}}')\right) =$

$$\left(\left(\begin{pmatrix} a'^{(Z\rightsquigarrow V)}_{1,1}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & a'^{(Z\rightsquigarrow V)}_{1,\mathfrak{n}}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(Z\rightsquigarrow V)}_{m_V,1}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{m_V,1} & & a'^{(Z\rightsquigarrow V)}_{m_V,\mathfrak{n}}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ a'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & a'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & a'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}+i\,\widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix},\right.$$

$$\left.\begin{pmatrix} b'^{(Z\rightsquigarrow V)}_{1,1}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & b'^{(Z\rightsquigarrow V)}_{1,\mathfrak{m}}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{1,\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ b'^{(Z\rightsquigarrow V)}_{m_V,1}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{m_V,1} & \cdots & b'^{(Z\rightsquigarrow V)}_{m_V,\mathfrak{m}}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ b'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & b'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & b'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}+i\,\widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right),$$

$$\left(\left(\begin{pmatrix} a'^{(V\rightsquigarrow Z)}_{1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(V\rightsquigarrow Z)}_{m_Z,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{m_Z,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{m_Z,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{m_Z,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{Z+1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{n}}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right),$$

$$\begin{pmatrix} b'^{(V\rightsquigarrow Z)}_{1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{1,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{m_V,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{m_V,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{m_V,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{m_V,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+1,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} = b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{m}} = b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1} = b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + i\ \widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{m}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{m}} = b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}.$$

With exactly the same way, this attack can be conducted against $\boldsymbol{U}$ node without the knowledge of node $\boldsymbol{V}$. Most of the times the sophistication of this attack is low to medium due to active orientation of this attack.

It is obvious that if the nodes have smooth valuations and smooth vulnerabilities, the following states applied during this attack:

$\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$	$\boldsymbol{\psi^{(U\rightsquigarrow V)}(t), \widehat{\psi}^{(V\rightsquigarrow V)}(t)}$
$\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) < 0}$	$\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) > 0}$
$\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) < 0}$	$\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) > 0}$
$\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) < 0}$	$\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) > 0}$
$\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) < \mathbf{0}}$	$\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) > 0}$
$\boldsymbol{\varphi^{(Z_{APT}\rightsquigarrow V)}(t) < 0}$	$\boldsymbol{\psi^{(Z_{APT}\rightsquigarrow V)}(t) > 0}$
$\boldsymbol{\varphi^{(V\rightsquigarrow Z_{APT})}(t) > 0}$	$\boldsymbol{\psi^{(V\rightsquigarrow Z_{APT})}(t) < 0}$
$\boldsymbol{\widehat{\varphi}^{(Z_{APT}\rightsquigarrow Z_{APT})}(t) > 0}$	$\boldsymbol{\widehat{\psi}^{(Z_{APT}\rightsquigarrow Z_{APT})}(t) < 0}$
$\boldsymbol{\varphi^{(Z_{APT}\rightsquigarrow U)}(t) < 0}$	$\boldsymbol{\psi^{(Z_{APT}\rightsquigarrow U)}(t) > 0}$
$\boldsymbol{\varphi^{(U\rightsquigarrow Z_{APT})}(t) > 0}$	$\boldsymbol{\psi^{(U\rightsquigarrow Z_{APT})}(t) < 0}$

5.3 APT Hunting Scenario 2

This second scenario APT hunting is a passive attack that consists in the monitoring of Cyber activity, often by covert means, escalates as follows. A family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \left\{\boldsymbol{\mathcal{Z}} = \boldsymbol{\mathcal{Z}}_{(\boldsymbol{Y},\boldsymbol{X})}(\boldsymbol{t}) = \left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}), (\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right)(\boldsymbol{t}) \in \left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}}\right)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I}\right\},$$

lying in (a partial danger sector $\mathcal{E} = \mathcal{E}_{\boldsymbol{U}\to\boldsymbol{V}}$ to) the node $\boldsymbol{V}$ from the node $\boldsymbol{Z}_{\boldsymbol{APT}} = \boldsymbol{Z}$ during the entire time set $\mathbb{I}$, is a **germ of (partial) passive attack from an intermediate node $\boldsymbol{Z}$ against the $(\boldsymbol{\kappa}_{\mathbf{1}}, \dots, \boldsymbol{\kappa}_{\boldsymbol{\lambda}})-$ resource parts $\boldsymbol{fr}\left(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa}_{\mathbf{1}}}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa}_{\mathbf{2}}}\right)$,…, $\boldsymbol{fr}\left(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa}_{\boldsymbol{\lambda}}}\right)$** of $\boldsymbol{V}$, during a given time subset $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathfrak{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathfrak{k}}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\right) =$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{a}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathbf{1}} & \cdots & \boldsymbol{a}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathbf{1}} & \cdots & \boldsymbol{a}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{b}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathbf{1}} & \cdots & \boldsymbol{b}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\mathbf{1},\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathbf{1}} & \cdots & \boldsymbol{b}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{V}}+\boldsymbol{\ell}_{\boldsymbol{V}},\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right)\right),$$

$$\left(\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{a}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\mathbf{1},\mathbf{1}} & \cdots & \boldsymbol{a}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\mathbf{1},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\mathbf{1},\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\boldsymbol{\ell}_{\boldsymbol{Z}},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\boldsymbol{\ell}_{\boldsymbol{Z}},\mathbf{1}} & \cdots & \boldsymbol{a}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\boldsymbol{\ell}_{\boldsymbol{Z}},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{Z}\rightsquigarrow\boldsymbol{Z})}_{\boldsymbol{\mathcal{M}}_{\boldsymbol{Z}}+\boldsymbol{\ell}_{\boldsymbol{Z}},\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right),\right.$$

$$\left(\begin{array}{ccc} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{b}^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1}+\boldsymbol{i}\ \hat{\boldsymbol{b}}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & \cdots & \boldsymbol{b}^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{m}}+\boldsymbol{i}\ \hat{\boldsymbol{b}}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1}+\boldsymbol{i}\ \hat{\boldsymbol{b}}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & \cdots & \boldsymbol{b}^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{m}}+\boldsymbol{i}\ \hat{\boldsymbol{b}}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right)\Bigg)\Bigg)\Bigg)$$

and is depicted, at a next moment $\boldsymbol{t'}=\boldsymbol{t}+\Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}'_{\mathbf{1}},\mathbb{w}'_{\mathbf{1}}),(\mathbb{z}'_{\mathbf{2}},\mathbb{w}'_{\mathbf{2}})\right)\in\left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}}\times\mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{Z}$ and $\boldsymbol{V}$ having the form

$$\left((\mathbb{z}'_{\mathbf{1}},\mathbb{w}'_{\mathbf{1}}),(\mathbb{z}'_{\mathbf{2}},\mathbb{w}'_{\mathbf{2}})\right)=$$

$$\left(\left(\left(\begin{array}{ccc} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+\boldsymbol{i}\ \widehat{\boldsymbol{\beta}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & & \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{array}\right),\right.\right.$$

$$\left.\left.\left(\begin{array}{ccc} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & & \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{array}\right)\right),$$

$$\left(\left(\begin{array}{ccc} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{array}\right)\right),$$

$$\left(\begin{array}{ccc} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & \cdots\cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} \\ \cdots & \cdots\cdots & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}}+i\ \widehat{b'}^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{array}\right)\Bigg)\Bigg)\Bigg).$$

With exactly the same way, this attack can be conducted against $\boldsymbol{U}$ node without the knowledge of node $\boldsymbol{V}$. Most of the times the sophistication of this attack is medium to high due to "passive" orientation of this.

Specifically, during this APT attack the following states applied:

$\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$	$\boldsymbol{\psi^{(U\rightsquigarrow V)}(t)\psi^{\varphi}, \widehat{\psi}^{(V\rightsquigarrow V)}(t)\ \psi^{c}}$
$\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t)=0}$	$\boldsymbol{\psi^{(U\rightsquigarrow V)}(t)=0}$
$\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t)=0}$	$\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t)=0}$
$\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t)=0}$	$\boldsymbol{\psi^{(V\rightsquigarrow U)}(t)=0}$
$\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t)=\mathbf{0}}$	$\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t)=0}$
$\boldsymbol{\varphi^{(Z\rightsquigarrow V)}(t)<0}$	$\boldsymbol{\psi^{(Z\rightsquigarrow V)}(t)>0}$
$\boldsymbol{\varphi^{(V\rightsquigarrow Z)}(t)=0}$	$\boldsymbol{\psi^{(V\rightsquigarrow Z)}(t)=0}$
$\boldsymbol{\widehat{\varphi}^{(Z\rightsquigarrow Z)}(t)>0}$	$\boldsymbol{\widehat{\psi}^{(Z\rightsquigarrow Z)}(t)<0}$
$\boldsymbol{\varphi^{(Z\rightsquigarrow U)}(t)<0}$	$\boldsymbol{\psi^{(Z\rightsquigarrow U)}(t)>0}$
$\boldsymbol{\varphi^{(U\rightsquigarrow Z)}(t)=0}$	$\boldsymbol{\psi^{(U\rightsquigarrow Z)}(t)=0}$

5.4 APT Hunting Scenario 3

In this scenario we actually have a highly sophisticated attack where intruder gains **access** to a device/system to which he has no right for access. Again here the node $\boldsymbol{U}$ is the APT actor that conducts the attack. During this attack the following general form of cyber-effect applies **[5]**:

$$\boldsymbol{g=g_t: \mathcal{Q}_5^{(V)}(U)(t)\rightarrow \mathcal{P}_{11}^{(U)}(V)(t')}$$

where $\boldsymbol{\mathcal{Q}_5^{(V)}(U)(t)}$ and $\boldsymbol{\mathcal{P}_{11}^{(U)}(V)(t')}$ are the combinatorial triplets

$\boldsymbol{Q_5^{(V)}(U)(t) = \left(\mathfrak{D}^{(fraction)}(U), \mathcal{S}_V\mathfrak{D}^{(fraction)}(U), \mathcal{U}_V\mathfrak{D}^{(fraction)}(U)\right)}$ and

$\boldsymbol{\mathcal{P}_{11}^{(U)}(V)(t') = \left(\mathfrak{D}_{available}^{(fraction)}(V), \mathcal{S}_U\mathfrak{D}_{available}^{(fraction)}(V), \mathcal{U}_U\mathfrak{D}_{available}^{(fraction)}(V)\right)}$,

respectively **([5]).**

In such a case, a family of coherent interactions

$$\boldsymbol{\mathcal{F} = \left\{\mathcal{Z} = \mathcal{Z}_{(Y,X)}(t) = \left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}_1', \mathbb{w}_1'), (\mathbb{z}_2', \mathbb{w}_2')\right)(t) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^4, t \in \mathbb{I}\right\}},$$

lying in (a partial danger sector $\mathcal{E} = \mathcal{E}_{U\to V}$ to) the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is a **germ of (partial) access attack against the $(\mu_1, \dots, \mu_\nu)$ − device parts $fr\left(dev_{\mu_1}^{(V)}\right), fr\left(dev_{\mu_2}^{(V)}\right), \dots, fr\left(dev_{\mu_\nu}^{(V)}\right)$ of V** during a given time subset $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $t \in \mathbb{I}$, the pair $\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^2$ of supervisory resource perceptions of U and V in the system of nodes U and V has the form

$$\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) =$$

$$\left(\left(\begin{pmatrix} a_{1,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{1,1}^{(V\rightsquigarrow V)} & \cdots & a_{1,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ a_{m_V,1}^{(W\rightsquigarrow V)} + i\ \hat{a}_{m_V,1}^{(V\rightsquigarrow V)} & \cdots & a_{m_V,\mathfrak{n}}^{(W\rightsquigarrow V)} + i\ \hat{a}_{m_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}, \right.\right.$$

$$\left.\left.\begin{pmatrix} b_{1,1}^{(U\rightsquigarrow V)} + i\ \hat{b}_{1,1}^{(V\rightsquigarrow V)} & \cdots & b_{1,\mathfrak{m}}^{(U\rightsquigarrow V)} + i\ \hat{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ b_{m_V,1}^{(U\rightsquigarrow V)} + i\ \hat{b}_{m_V,1}^{(V\rightsquigarrow V)} & \cdots & b_{m_V,\mathfrak{m}}^{(U\rightsquigarrow V)} + i\ \hat{b}_{m_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right)\right),$$

$$\left(\begin{pmatrix} a_{1,1}^{(V\rightsquigarrow U)} + i\ \hat{a}_{1,1}^{(U\rightsquigarrow U)} & \cdots & a_{1,\mathfrak{n}}^{(V\rightsquigarrow U)} + i\ \hat{a}_{1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots & \cdots \\ a_{m_U,1}^{(V\rightsquigarrow U)} + i\ \hat{a}_{m_U,1}^{(U\rightsquigarrow U)} & \cdots & a_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)} + i\ \hat{a}_{m_U,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right),$$

$$\left(\begin{matrix} \boldsymbol{b}_{1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{m}}^{(U\rightsquigarrow U)} \\ \cdots \\ \boldsymbol{b}_{m_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{b}_{m_U,\mathfrak{m}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,\mathfrak{m}}^{(U\rightsquigarrow U)} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right)\Bigg)\Bigg)\Bigg)$$

and is depicted, at a next moment $\boldsymbol{t'}=\boldsymbol{t}+\Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\mathbf{1}}',\mathbb{w}_{\mathbf{1}}'),(\mathbb{z}_{\mathbf{2}}',\mathbb{w}_{\mathbf{2}}')\right)\in\left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}}\times\mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form $\left((\mathbb{z}_{\mathbf{1}}',\mathbb{w}_{\mathbf{1}}'),(\mathbb{z}_{\mathbf{2}}',\mathbb{w}_{\mathbf{2}}')\right)=$

$$\left(\left(\left(\begin{matrix} \boldsymbol{a'}_{1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & \boldsymbol{a'}_{1,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots \\ \boldsymbol{a'}_{m_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,1} & & \boldsymbol{a'}_{m_V,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right),\right.\right.$$

$$\left.\left.\left(\begin{matrix} \boldsymbol{b'}_{1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & \boldsymbol{b'}_{1,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{1,\mathfrak{m}} \\ \cdots \\ \boldsymbol{b'}_{m_U,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{m_U,1} & \cdots & \boldsymbol{b'}_{m_U,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{m_U,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right)\right)\right),$$

$$\left(\begin{matrix} \boldsymbol{a'}_{1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{1,1}=\boldsymbol{a'}_{1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & \boldsymbol{a'}_{1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{1,\mathfrak{n}}=\boldsymbol{a'}_{1,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots \\ \boldsymbol{a'}_{m_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{m_U,1}=\boldsymbol{a'}_{m_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,1} & \cdots & \boldsymbol{a'}_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{m_U,\mathfrak{n}}=\boldsymbol{a'}_{m_V,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ \boldsymbol{a'}_{m_V+1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V+1,1} & & \boldsymbol{a'}_{m_V+1,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a'}_{m_V+\lambda,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V+\lambda,1} & & \boldsymbol{a'}_{m_V+\lambda,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V+\lambda,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right),$$

$$\begin{pmatrix} b'^{(V\nrightarrow U)}_{1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,1} = b'^{(U\nrightarrow V)}_{1,1} + i\ \widehat{b}'^{(V\nrightarrow V)}_{1,1} & \cdots & b'^{(V\nrightarrow U)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,\mathfrak{n}} = b'^{(U\nrightarrow V)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(V\nrightarrow V)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\nrightarrow U)}_{m_U,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,1} = b'^{(U\nrightarrow V)}_{m_V,1} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V,1} & \cdots & b'^{(V\nrightarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,\mathfrak{n}} = b'^{(U\nrightarrow V)}_{m_V,\mathfrak{n}} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V,\mathfrak{n}} \\ b'^{(U\nrightarrow V)}_{m_V+1,1} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V+1,1} & \cdots & b'^{(U\nrightarrow V)}_{m_V+1,\mathfrak{n}} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ b'^{(U\nrightarrow V)}_{m_V+\lambda,1} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V+\lambda,1} & \cdots & b'^{(U\nrightarrow V)}_{m_V+\lambda,\mathfrak{n}} + i\ \widehat{b}'^{(V\nrightarrow V)}_{m_V+\lambda,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}.$$

Most of the times the sophistication of this attack is medium to high. Specifically, during this scenario the following states applied:

$\boldsymbol{\varphi^{(U\nrightarrow V)}(t), \widehat{\varphi}^{(V\nrightarrow V)}(t)}$	$\boldsymbol{\psi^{(U\nrightarrow V)}(t), \widehat{\psi}^{(V\nrightarrow V)}(t)}$
$\boldsymbol{\varphi^{(U\nrightarrow V)}(t) < 0}$	$\boldsymbol{\psi^{(U\nrightarrow V)}(t) > 0}$
$\boldsymbol{\widehat{\varphi}^{(V\nrightarrow V)}(t) = 0}$	$\boldsymbol{\widehat{\psi}^{(V\nrightarrow V)}(t) = 0}$
$\boldsymbol{\varphi^{(V\nrightarrow U)}(t) = 0}$	$\boldsymbol{\psi^{(V\nrightarrow U)}(t) = 0}$
$\boldsymbol{\widehat{\varphi}^{(U\nrightarrow U)}(t) > 0}$	$\boldsymbol{\widehat{\psi}^{(U\nrightarrow U)}(t) < 0}$

Proposition 5.1 It is clear that during this scenario the attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U}$ that plays the role of APT actor against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})-$ device parts $\boldsymbol{fr\left(dev^{(V)}_{\mu_1}\right)}$, $\boldsymbol{fr\left(dev^{(V)}_{\mu_2}\right)}$,…, $\boldsymbol{fr\left(dev^{(V)}_{\mu_\nu}\right)}$ of $\boldsymbol{V}$, the following elementary properties hold.

i. The (Euclidean) norm $\left\| \boldsymbol{a'^{(U\nrightarrow V)}} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is less than the (Euclidean) norm $\left\|\boldsymbol{a^{(U\nrightarrow V)}}\right\|$ of the initial overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of$\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{a'^{(U\nrightarrow V)}} \right\| < \left\|\boldsymbol{a^{(U\nrightarrow V)}}\right\|.$$

ii. The (Euclidean) norm $\left\| \boldsymbol{b'^{(U\nrightarrow V)}} \right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is greater than the (Euclidean) norm $\left\|\boldsymbol{b^{(U\nrightarrow V)}}\right\| := \left(\sum_{j=1}^{\mathfrak{m}} \sum_{\lambda=1}^{\ell_V} \left|\boldsymbol{b^{(U\nrightarrow V)}_{\mathcal{M}_U+\lambda,j}}\right|^2\right)^{1/2}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{b'^{(U\nrightarrow V)}} \right\| > \left\|\boldsymbol{b^{(U\nrightarrow V)}}\right\|.$$

iii. The (Euclidean) norm $\left\|\widehat{\boldsymbol{a}}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is greater than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{a}}^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{a}^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{\beta}}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\| > \boldsymbol{max}\left\{\left\|\widehat{\boldsymbol{\beta}}^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\|, \left\|\boldsymbol{\beta}^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\|\right\}.$$

iv. The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is less than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{b}^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\|, \left\|\boldsymbol{b}^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\|\right\}. \blacksquare$$

Remark 5.2 Of course, in the special case where there is a fully successful access attack the following hold:

$$\left\|\boldsymbol{a}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\| \approx \boldsymbol{0}, \left\|\boldsymbol{a}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{U})}\right\| = \sqrt{\boldsymbol{m_U}}, \left\|\boldsymbol{b}'^{(\boldsymbol{U}\nrightarrow\boldsymbol{V})}\right\| = \sqrt{\boldsymbol{m_U}}. \blacksquare$$

An access attack, besides a reflexive homomorphism, can take place **physically** when an attacker $\boldsymbol{U}$, physically gains access of victim node devices $\boldsymbol{V}$.

5.5 APT Hunting Scenario 4

In this scenario the actual attack vector which involves is an unauthorized detection mapping and services to steal data. This attack can potentially take place both actively and passively. Specifically, in passive scenario 4, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture. In active scenario, the intruder engages with the target system through methods like port scans. Again here the node that plays the role of the APT actor is the $\boldsymbol{U}$**.**

Thus, during this attack the following general form of cyber-effect applies:

$$\boldsymbol{g} = \boldsymbol{g_t}\colon \boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U})(\boldsymbol{t}) \to \boldsymbol{\mathcal{P}_7^{(U)}}(\boldsymbol{V})(\boldsymbol{t}')$$

where $\boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U})(\boldsymbol{t}')$ and $\boldsymbol{\mathcal{P}_7^{(U)}}(\boldsymbol{V})(\boldsymbol{t}')$ are the combinatorial triplets

$$\boldsymbol{\mathcal{Q}_9^{(V)}(U) = \mathcal{Q}_9^{(V)}(U)(t') = (\mathfrak{R}_{available}(V), \mathcal{S}_U\mathfrak{R}_{available}(V), \mathcal{U}_U\mathfrak{R}_{available}(V)\ )}$$

and

$$\boldsymbol{\mathcal{P}_7^{(U)}(V)(t') = (\mathfrak{C}_{available}(V), \mathcal{S}_U\mathfrak{C}_{available}(V), \mathcal{U}_U\mathfrak{C}_{available}(V)\ )}$$

respectively **([5]).**

It is obvious that the purpose of this attack is for node $\boldsymbol{U}$ to uncover all constituents' vulnerabilities of node $\boldsymbol{V}$.

A family of coherent interactions

$$\boldsymbol{\mathcal{F} = \left\{\mathcal{Z} = \mathcal{Z}_{(Y,X)}(t) = \left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\right)(t) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^4, t \in \mathbb{I}\right\},}$$

lying in (the partial danger sector $\mathcal{E} = \mathcal{E}_{U\to V}$ to) the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is **a germ of scenario 4 attack against the $(\mu_1, \dots, \mu_\nu)-$ device parts $fr\left(dev_{\mu_1}^{(V)}\right)$, $fr\left(dev_{\mu_2}^{(V)}\right)$,..., $fr\left(dev_{\mu_\nu}^{(V)}\right)$ and the $(\kappa_1, \dots, \kappa_\lambda)-$ resource parts $fr\left(res_{\kappa_1}^{(V)}\right)$, $fr\left(res_{\kappa_2}^{(V)}\right)$,..., $fr\left(res_{\kappa_\lambda}^{(V)}\right)$ of V** during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $t \in \mathbb{I}$, the pair $\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^2$ of supervisory constituents perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) =$$

$$\left(\left(\left(\begin{array}{ccc} \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ \dots & & \dots \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ a_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & a_{\mathcal{M}_V+1,\mathfrak{n}}^{(U\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \dots & & \dots \\ a_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & a_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(U\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ \dots & & \dots \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \end{array}\right),\right.\right.$$

$$\left.\left.\left(\begin{array}{ccc} \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ \dots & & \dots \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ b_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & b_{\mathcal{M}_V+1,\mathfrak{m}}^{(U\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \dots & & \dots \\ b_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & b_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(U\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \\ \dots & & \dots \\ \mathbf{0} & \dots\dots\dots & \mathbf{0} \end{array}\right)\right),$$

$$\left(\left(\begin{array}{ccc} \boldsymbol{a}_{1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{a}_{1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{a}_{m_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{a}_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{a}_{\mathcal{M}_U+1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_U+1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{a}_{\mathcal{M}_U+1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_U+1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{a}_{\mathcal{M}_U+\ell_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_U+\ell_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{a}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right),\right.$$

$$\left.\left(\begin{array}{ccc} \boldsymbol{b}_{1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{b}_{m_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{b}_{\mathcal{M}_U+1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{\mathcal{M}_U+1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{b}_{\mathcal{M}_U+\ell_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+\ell_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right)\right)\right)$$

and is depicted, at a next moment $\boldsymbol{t'}=\boldsymbol{t}+\Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\boldsymbol{1}}',\mathbb{w}_{\boldsymbol{1}}'),(\mathbb{z}_{\boldsymbol{2}}',\mathbb{w}_{\boldsymbol{2}}')\right)\in\left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}}\times\mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\boldsymbol{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form $\left((\mathbb{z}_{\boldsymbol{1}}',\mathbb{w}_{\boldsymbol{1}}'),(\mathbb{z}_{\boldsymbol{2}}',\mathbb{w}_{\boldsymbol{2}}')\right)=$

$$\left(\left(\left(\begin{array}{ccc} \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{a'}_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & \boldsymbol{a'}_{\mathcal{M}_V+1,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right),\right.\right.$$

$$\left.\left.\left(\begin{array}{ccc} \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{b'}_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & & \boldsymbol{b'}_{\mathcal{M}_V+1,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right)\right)\right)$$

$$\begin{pmatrix} \begin{pmatrix} a'^{(V\nrightarrow U)}_{1,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{1,1} \\ \cdots \\ a'^{(V\nrightarrow U)}_{m_U,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{m_U,1} \\ \cdots \\ 0 \\ \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ 0 \\ \cdots \\ 0 \end{pmatrix} & \cdots\cdots\cdots & \begin{pmatrix} a'^{(V\nrightarrow U)}_{1,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{1,\mathfrak{n}} \\ \cdots \\ a'^{(V\nrightarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{m_U,\mathfrak{n}} \\ \cdots \\ 0 \\ \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ 0 \\ \cdots \\ 0 \end{pmatrix} \end{pmatrix},$$

$$\begin{pmatrix} \begin{pmatrix} b'^{(V\nrightarrow U)}_{1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,1} \\ \cdots \\ b'^{(V\nrightarrow U)}_{m_U,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,1} \\ b'^{(V\nrightarrow U)}_{m_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+1,1} \\ \cdots \\ b'^{(V\nrightarrow U)}_{m_U+\ell_V,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+\ell_V,1} \\ 0 \\ \cdots \\ 0 \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,1} \\ \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,1} \\ 0 \\ \cdots \\ 0 \end{pmatrix} & \cdots\cdots\cdots & \begin{pmatrix} b'^{(V\nrightarrow U)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,\mathfrak{n}} \\ \cdots \\ b'^{(V\nrightarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,\mathfrak{n}} \\ b'^{(V\nrightarrow U)}_{m_U+1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+1,\mathfrak{n}} \\ \cdots \\ b'^{(V\nrightarrow U)}_{m_U+\ell_V,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+\ell_V,n} \\ 0 \\ \cdots \\ 0 \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,n} \\ \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,n} \\ 0 \\ \cdots \\ 0 \end{pmatrix} \end{pmatrix}.$$

Most of the times the sophistication of this attack is very low and highly "transparent" to attacked node. Frequently, after this attack a more sophisticated attack is expected. Specifically, during scenario 4 attack the following states applied:

$\varphi^{(U\nrightarrow V)}(t), \widehat{\varphi}^{(V\nrightarrow V)}(t)$	$\psi^{(U\nrightarrow V)}(t), \widehat{\psi}^{(V\nrightarrow V)}(t)$
$\varphi^{(U\nrightarrow V)}(t) < 0$	$\psi^{(U\nrightarrow V)}(t) > 0$
$\widehat{\varphi}^{(V\nrightarrow V)}(t) = 0$	$\widehat{\psi}^{(V\nrightarrow V)}(t) = 0$
$\varphi^{(V\nrightarrow U)}(t) = 0$	$\psi^{(V\nrightarrow U)}(t) = 0$
$\widehat{\varphi}^{(U\nrightarrow U)}(t) > 0$	$\widehat{\psi}^{(U\nrightarrow U)}(t) < 0$

Proposition 5.2 It is obvious that during this attack $\mathcal{F}$ from $\boldsymbol{U}$ against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu}) -$ resource parts $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\mu_1}}^{(V)}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\mu_2}}^{(V)}\right), \dots, \boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\mu_\nu}}^{(V)}\right)$ of $\boldsymbol{V}$, the following elementary properties hold:

i. The (Euclidean) norm $\left\| \boldsymbol{a}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is much less than the (Euclidean) norm $\left\|\boldsymbol{a}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|$ of the initial overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{a}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})} \right\| \ll \left\|\boldsymbol{a}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|.$$

ii. The (Euclidean) norm $\left\| \boldsymbol{b}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})} \right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is much greater than the (Euclidean) norm $\left\|\boldsymbol{b}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\| := \left(\sum_{j=1}^{\mathfrak{m}} \sum_{\lambda=1}^{\boldsymbol{\ell_V}} \left|\boldsymbol{b}_{\boldsymbol{\mathcal{M}_U}+\boldsymbol{\lambda},\boldsymbol{j}}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right|^2\right)^{\boldsymbol{1/2}}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{b}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})} \right\| \gg \left\|\boldsymbol{b}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|.$$

iii. The (Euclidean) norm $\left\|\widehat{\boldsymbol{a}}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is much greater than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{a}}^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{a}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{a}}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\| \gg \boldsymbol{max}\left\{\left\|\widehat{\boldsymbol{a}}^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\|, \left\|\boldsymbol{a}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|\right\}.$$

iv. The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is less than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{b}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U} \nrightarrow \boldsymbol{U})}\right\|, \left\|\boldsymbol{b}^{(\boldsymbol{U} \nrightarrow \boldsymbol{V})}\right\|\right\}. \blacksquare$$

The criticality of this attack is high since most of times it is the omen of a more severe or more sophisticated attack.

5.6 APT Hunting Scenario 5

In this scenario we orient 2 attacks that intent to sophisticatedly deny services and generally resources to authorized users. The attacker $\boldsymbol{U}$ that again plays the role of the APT actor makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine. The difference between these 2 types of attacks is actually the source. In the first type the attack is initiated by only one node. On the other hand, the second vector has the engagement of a multitude of nodes (intentionally or not, e.g. via Botnets).

Thus, during this kind of attack the following general form of cyber-effect applies:

$$\boldsymbol{g = g_t : Q_9^{(V)}(U)(t) \to \mathcal{P}_9^{(U)}(V)(t')}$$

where $\boldsymbol{Q_9^{(V)}(U)(t')}$ **and** $\boldsymbol{\mathcal{P}_9^{(U)}(V)(t')}$ are the combinatorial triplets

$$\boldsymbol{Q_9^{(V)}(U) = Q_9^{(V)}(U)(t') = (\mathfrak{R}_{available}(V), \mathcal{S}_U\mathfrak{R}_{available}(V), \mathcal{U}_U\mathfrak{R}_{available}(V))}$$

and

$$\boldsymbol{\mathcal{P}_9^{(U)}(V)(t') = (\mathfrak{R}_{available}(V), \mathcal{S}_U\mathfrak{R}_{available}(V), \mathcal{U}_U\mathfrak{R}_{available}(V))}$$

respectively ([5]).

It is obvious that the purpose of this attack is for node $\boldsymbol{U}$ to keep all resources/services of node $\boldsymbol{V}$ busy in order to make them unavailable to all users that really need them.

A family of coherent interactions

$$\boldsymbol{\mathcal{F} = \{\mathcal{Z} = \mathcal{Z}_{(Y,X)}(t) = ((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2))(t) \in (\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k})^4, t \in \mathbb{I}\}},$$

lying in the partial danger sector $\mathcal{E} = \mathcal{E}_{U\to V}$ to the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is a **germ of scenario 5 attack against the** $\boldsymbol{(\mu_1, \dots, \mu_v) - fr\left(dev_{\mu_2}^{(V)}\right), \dots, fr\left(dev_{\mu_v}^{(V)}\right)}$ **resource parts** $\boldsymbol{fr\left(res_{\kappa_1}^{(V)}\right)}$, $\boldsymbol{fr\left(res_{\kappa_2}^{(V)}\right), \dots, fr\left(res_{\kappa_\lambda}^{(V)}\right)}$ **of** $\boldsymbol{V}$ during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\boldsymbol{((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)) \in (\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k})^2}$ of supervisory constituents perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\right) =$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{a}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,1} \\ \cdots \\ \boldsymbol{a}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{a}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots \\ \boldsymbol{a}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{b}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,1} \\ \cdots \\ \boldsymbol{b}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{b}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots \\ \boldsymbol{b}^{(U \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right)\right),$$

$$\left(\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{a}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ \boldsymbol{a}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{a}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots \\ \boldsymbol{a}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{b}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ \boldsymbol{b}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \\ \\ \cdots \cdots \cdots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ \boldsymbol{b}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} \\ \cdots \\ \boldsymbol{b}^{(V \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right)\right)\right)$$

and is depicted, at a next moment $\boldsymbol{t}' = \boldsymbol{t} + \Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form

$$\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) =$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ a'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+i\ \widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1}=0 \\ \cdots \\ a'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+i\ \widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}=0 \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \cdots\cdots \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ a'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}}+i\ \widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}}=0 \\ \cdots \\ a'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}+i\ \widehat{a}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}=0 \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ b'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1}+i\ \widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1}=1 \\ \cdots \\ b'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}+i\ \widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1}=1 \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \cdots\cdots \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ b'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}}+i\ \widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}}=1 \\ \cdots \\ b'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}+i\ \widehat{b}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}=1 \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right)\right),$$

$$\left(\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ a'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1}+i\ \widehat{a}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ a'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1}+i\ \widehat{a}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \cdots\cdots \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ a'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}}+i\ \widehat{a}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots \\ a'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}+i\ \widehat{a}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1}+i\ \widehat{b}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} \\ \cdots \\ b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1}+i\ \widehat{b}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix} \cdots\cdots \begin{matrix} \mathbf{0} \\ \cdots \\ \mathbf{0} \\ b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}}+i\ \widehat{b}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} \\ \cdots \\ b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}}+i\ \widehat{b}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} \\ \mathbf{0} \\ \cdots \\ \mathbf{0} \end{matrix}\right)\right)\right).$$

During this attack the results depicted in previous matrices are usually temporary and only strictly during the application of the attack. Most of the times the sophistication of this attack is very low and highly "transparent" to attacked node since the lack of resources is more than obvious. Frequently, after or during this attack a more sophisticated attack is expected. Specifically, during these attacks the following states applied:

$$\boldsymbol{\varphi}^{(U\rightsquigarrow V)}(t), \widehat{\boldsymbol{\varphi}}^{(V\rightsquigarrow V)}(t) \qquad \boldsymbol{\psi}^{(U\rightsquigarrow V)}(t), \widehat{\boldsymbol{\psi}}^{(V\rightsquigarrow V)}(t)$$

$\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) < 0}$	$\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) > 0}$
$\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) < 0}$	$\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) > 0}$
$\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) > 0}$	$\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) < 0}$
$\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) > 0}$	$\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) < 0}$

Proposition 5.3 It is obvious that during this scenario's attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U}$ against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_v})-$ resource parts $\boldsymbol{fr\left(res_{\mu_1}^{(V)}\right)}$, $\boldsymbol{fr\left(res_{\mu_2}^{(V)}\right)}$,…, $\boldsymbol{fr\left(res_{\mu_v}^{(V)}\right)}$ of $\boldsymbol{V}$, the following elementary properties hold:

i. The (Euclidean) norm $\left\| \boldsymbol{a'^{(U\rightsquigarrow V)}} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is temporary $\boldsymbol{0}$:

$$\left\| \boldsymbol{a'^{(U\rightsquigarrow V)}} \right\| = \boldsymbol{0}.$$

ii. The (Euclidean) norm $\left\| \boldsymbol{b'^{(U\rightsquigarrow V)}} \right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is temporary $\boldsymbol{1}$:

$$\left\| \boldsymbol{b'^{(U\rightsquigarrow V)}} \right\| = \boldsymbol{1}.$$

iii. The (Euclidean) norm $\left\| \boldsymbol{\widehat{a}'^{(U\rightsquigarrow U)}} \right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is much greater than the (Euclidean) norms

$$\left\| \boldsymbol{\widehat{a}^{(U\rightsquigarrow U)}} \right\| \text{ and } \left\| \boldsymbol{a^{(U\rightsquigarrow V)}} \right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{\widehat{\beta}'^{(U\rightsquigarrow U)}} \right\| \geq \boldsymbol{max}\left\{ \left\| \boldsymbol{\widehat{\beta}^{(U\rightsquigarrow U)}} \right\|, \left\| \boldsymbol{\beta^{(U\rightsquigarrow V)}} \right\| \right\}.$$

iv. The (Euclidean) norm $\left\| \boldsymbol{\widehat{b}'^{(U\rightsquigarrow U)}} \right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is less than the (Euclidean) norms

$$\left\| \boldsymbol{\widehat{b}^{(U\rightsquigarrow U)}} \right\| \text{ and } \left\| \boldsymbol{b^{(U\rightsquigarrow V^{\prime\prime})}} \right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{\widehat{b}'^{(U\rightsquigarrow U)}} \right\| < \boldsymbol{min}\left\{ \left\| \boldsymbol{\widehat{b}^{(U\rightsquigarrow U)}} \right\|, \left\| \boldsymbol{b^{(U\rightsquigarrow V)}} \right\| \right\}. \blacksquare$$

The importance of this attack is high since most of the time, especially during distributed one, the nodes that participate are already compromised via Access attack that has already discussed.

References

[1]. Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?

[2]. https://attack.mitre.org/resources/enterprise-introduction/ ATT&CK for Enterprise Introduction

[3]. Daras, N.J.: *On the mathematical definition of cyberspace*, Theoretical Mathematics & Applications, vol.8, no.1, 2018, 9-45, , Scienpress Ltd, 2018

[4]. Daras, N.J and Alexopoulos, A.: *Mathematical description of cyber-attacks and proactive defenses*, Journal of Applied Mathematics & Bioinformatics, vol.7, no.1, 2017, pp. 71-142

[5]. Daras, N.J and Alexopoulos, A.: *Modeling Cyber-Security*, Journal of Applied Mathematics & Bioinformatics, vol.7, no.1, 2017, pp. 71-142

[6]. Alexopoulos, A. and Daras, N.: Mathematical Study of Various Types of Cyber-Attacks and Protection, Journal of Computations & Modelling, vol.8, no.2, 2018