Novel Vulnerability Metrics for Interdependent System based on System Controllability

L Faramondi, G Oliva and V Piemonte

University Campus Bio-Medico di Roma, Faculty of Engineering, via Álvaro del Portillo 21, 00128, Rome, Italy.

Abstract. In this paper we develop novel vulnerability metrics for interdependent critical infrastructures or economic sectors based on the concept of controllability. Specifically, we consider the Input-Output Inoperability Model, that represents the dynamics of the dependencies and interdependencies among infrastructures or sectors during an adverse event or malicious attack, and we argue that the more the system is controllable via an external perturbation that represents the fault or attack, the more the system is vulnerable. Therefore, we analyze the vulnerability of the system in terms of the magnitude of the associated controllability matrix. Moreover, based on the proposed index, we develop a simple defensive strategy to reduce the effect of an attack. A validation of the approach with respect to real data concludes the paper.

1. Introduction

Due to the diffusion of emerging technologies (e.g., cloud services, IoT systems and mobile computing), modern infrastructures or economic sectors are now part of the same macro-system; since their functionalities are essential to the health, safety, security or economic well-being of a nation or community, such an increased degree of mutual dependency is both a blessing and a curse. In fact, from one side the increasing degree of cooperation among sectors or infrastructures is improving the quality of our everyday life; however, from another side, the growing dependency of such systems on each other is posing a serious threat to our society, because of the possibility of cascading effects in the event of a natural disaster, human error or terroristic attack.

In this view, control theory represents a valuable framework for analyzing such systems, since such a discipline provides useful tools and methodologies to deal with dynamical systems, disturbances, model uncertainties, feedback and interdependency. Among other ideas, the concept of controllability appears particularly valuable to quantify the effect of the propagation of faults and cascading events [1, 2, 3].

Consider an attacker aiming at disrupting the services and the functioning of a group of densely interrelated critical infrastructures or sectors; in this perspective, the ability of the attacker to control the system can be regarded as highly disruptive.

We point out that, in the literature, the relation between control and attacks has been widely investigated. In the context of Cyber Physical Systems, in [4] the authors face the problem of identifying a set of driver nodes, i.e., nodes in a network that guarantee the structural controllability of a system. The relation between attack vulnerability and controllability has been also studied in [5], where the authors analyze the effect of node deletion from a graph representing the structure of an
interconnected system, following several attack strategies and considering different network topologies. A similar topological approach has been adopted in [6] to study the robustness of power grids to node or edge disruption or in [7, 8, 9, 10], where vulnerable nodes are identified via optimization techniques. In [11] random attacks or faults have been regarded as a major cause of damage to interconnected networks. An interesting study about the relation between the attacks and controllability of networks is presented by Liu et al. [12]; in this work, the authors show that network controllability can be conveniently studied in the framework of percolation theory. Finally, in [13] possible countermeasures are investigated considering a network of networks scenario.

In this paper we develop a new metric able to highlight the fragility of a subset of interdependent systems, services, or sectors, based on the controllability of the system, with particular reference to the Input Output Inoperability Model [14, 15, 16]. In order to show the effectiveness of the proposed index, we compare it with well established descriptors of the vulnerability of such a model. Moreover, we develop a strategy to guide the defense of the different sectors in order to achieve an arbitrarily small value of the proposed index.

The outline of the paper is as follows: In Section 2 we provide some preliminary definitions; in Section 3 we provide a short description about the input output models with a focus on the Inoperability Input Output model; the definition of the new metric and the novel defensive strategy are discussed in Section 4; results and discussions are collected in Section 5 with the aim to validate the proposed index; finally, some conclusive remarks are collected in Section 6.

2. Preliminaries

2.1. General preliminaries

In the following, we denote by $\text{card}(X)$ the cardinality of a set $X$. Moreover, we denote matrices and vectors via cursive letters, and we use $k_m$ to indicate a vector in $\mathbb{R}^m$ whose components are all equal to $k$. We represent by $||A||_1$ the entrywise 1-norm of an $n \times n$ matrix $A$, i.e.,

$$||A||_1 = \sum_{i=1}^n \sum_{j=1}^n |a_{ij}|.$$  

(1)

2.2. LTI dynamic system controllability

Let a continuous-time linear time-invariant (LTI) system having the form

$$x(t) = Ax(t) + Bu(t),$$

(2)

where $x \in \mathbb{R}^n$ represents the state variable vector, $u \in \mathbb{R}^p$ is the input vector, $A$ is the $n \times n$ dynamic matrix having constant entries $a_{ij}$, and $B$ is the $n \times p$ input matrix, having entries $b_{ij}$. The above system is controllable in for any finite time window $[t_0, T]$ we can find an input signal $u(t)$ for $t \in [t_0, T]$ able to steer the state $x(t)$ from any initial value to any final value.

According to Kalman [17], System (2) is controllable if and only if the controllability matrix

$$R = [B \ AB \ldots \ A^{n-1}B]$$

(3)

is full row-rank, i.e., $\text{ifrank} (R) = n$. Notice that, $\text{ifrank} (R) = q < n$, then the state space $\mathbb{R}^n$ can be decomposed in a controllable subspace of dimension $q$ and an uncontrollable subspace of $n - q$.

3. Inoperability input output model

The traditional Input Output Model is a popular static equilibrium model to represent macroeconomic interaction among the economic sectors of a country or region. Such a tool is often used to describe the growth of an economy due to sector expansion or technology adoption [18, 19]. More in detail, let us consider the model defined by Equation 4 for interconnected industry sectors (e.g., transportations, manufacturing, retail trade, etc.); vector $x \in \mathbb{R}^n$ represents the set of production outputs of each sector, while vector $c \in \mathbb{R}^n$ represents the set of consumer demand for goods, services, and usage in each sector; finally, the $n \times n$ matrix $A$ is the so-called Leontief matrix whose elements $a_{ij}$ (Leontief technical coefficients) represent the ratio of the output produced by the $i$-th infrastructure that is required by the $j$-th infrastructure in order to generate one unit of production. In a nutshell, the

2
Input-Output Model reads as follows:

\[ x = Ax + c. \] (4)

Note that Equation (4) captures the equilibrium between demand and production at the different sectors and describes how industry output (\(x\)) is a function of intermediate demand (\(Ax\)) among sectors and final demand (\(c\)).

Following the economic equilibrium theory of Leontief [18, 19], a static Demand-Reduction Model for \(n\) industrial sectors is given by:

\[ \Delta x = A\Delta x + \Delta c, \] (5)

where \(\Delta x\) represents the difference between the planned \((x_0)\) and the degraded production \((x_d)\), \(\Delta c\) is the difference between the planned final demand \((c_0)\) and the degraded final demand \((c_d)\).

Based on the latter model, in [14] a model able to capture the dependency between sectors or infrastructures is developed, by introducing the notion of inoperability on an infrastructure/sector, i.e., its inability (as a percentage) to operate properly due to the degraded production.

Let \(q \in \mathbb{R}^n\) be the vector whose entries \((q_i)\) represent the inoperability of the \(i\)-th sector. With the aim to describe how inoperability propagates, [14] introduces an \(n \times n\) transformation matrix

\[ P = [\text{diag}(x_0)]^{-1}. \] (6)

The inoperability is then computed by applying the transformation to Equation (5), i.e.,

\[ q = P\Delta x. \] (7)

The outcome of such a transformation is the Input Output Inoperability Model (IIM) [15, 16]

\[ q = A^*q + c^* \Rightarrow q = (I - A^*)^{-1}c^* = D^*c^*, \] (8)

where \(A^* = PAP^{-1}\), and \(c^* = P\Delta c\). In this view, vector \(c^*\) describes the perturbation in demand resulting from a disruptive event, and is the driver of inoperability in the demand-reduction, while \(A^*\) is the interdependency matrix, which can be derived from economic data as in [20], or using other sources as in [21].

In [14] the static IIM defined in Equation 8 is further extended by introducing a dynamics, i.e.,

\[ \dot{q}(t) = K(A^* - I)q(t) + Kc^*(t), \] (9)

where matrix \(K\) is the industry resilience coefficient matrix (it has a relation with the convergence rate towards an equilibrium), and each element \(k_{ii}\) measures the resilience of the \(i\)-th infrastructure. The \(k_{ii}\) coefficient can also be seen as the recovery rate with respect to adverse or malicious events. In the absence of concrete information, it is common practice to set \(K = I\).

3.1 Key sectors and criticality measures for IIM

Analogously to component importance measures (CIMs) in the reliability engineering literature, key sector analysis is used in the economic input-output literature to identify the criticality that certain industry sectors have on the economy, and the productivity of a country or region. In the literature, two indices for expressing the criticality of an infrastructure within a given scenario have been introduced in [22, 23], based on their economic input-output counterpart [24, 25]. These two indices are referred to here as the dependency index, and the influence gain.

The dependency index is defined as the sum of the coefficients of matrix \(A^*\) along a row, shown in

\[ \delta_i = \sum_{j=1}^{n} a^*_{ij}. \] (10)

The dependency index measures the robustness of the \(i\)th infrastructure with respect to the inoperability of the other infrastructures, representing a measure of the residual operational capability of the \(i\)th infrastructure when every other infrastructure is fully inoperable. The lower the value, the greater the ability of the \(i\)th infrastructure to maintain functionality despite the inoperability of the other sectors upon which it relies. On the other side, \(\delta_i \geq 1\) means that the operability of the \(i\)th infrastructure might be nullified even if the other infrastructures still have some residual operational capability.

Another index, the influence gain, measures the influence that one infrastructure exerts over the other infrastructures. It is defined as the sum of the coefficients of matrix \(A^*\) along a column, as in
(11).

\[ \gamma_i = \sum_{j=1}^{n} a_{ji} \]  

A large influence gain suggests that the inoperability of the \( i \)-th infrastructure induces significant degradations on the entire system. When \( \gamma_i > 1 \), the adverse effects in terms of inoperability induced by cascading phenomena on the other infrastructures are amplified.

Ordering the sectors in decreasing order of \( \delta_i \) provides a ranking of sectors that are most impacted by inoperability in other sectors, and likewise, a decreasing order of \( \gamma_i \) results in a ranking of sectors that are most impactful on other sectors. In a more absolute measure, Hirschmann [26] suggests that key sectors are those sectors for which the normalized version of indices (10) and (11) are greater than 1.

4. IIM vulnerability/robustness metrics based on controllability

In this section we develop novel vulnerability/robustness metrics of the IIM model that are based on the concept of controllability. In fact, in this section we argue that the more an IIM system is controllable by means of the input \( c^*(t) \), the more an adverse event or a terroristic attack may have severe consequences on the overall system.

Let us consider a dynamic IIM model as din Equation (9), and for the sake of simplicity suppose that it holds

\[ c^*(t) = B f(t), \]  

where \( f(t) \) is a scalar input that represents an attack signal, and \( B \) is a column vector whose entries \( b_i \) model the vulnerability of the \( i \)-th infrastructure to an attack or failure affecting it directly. In more details, we define the entries \( b_i \) in the range \([0 \ldots 1]\), where \( b_i = 0 \) represents an infrastructure that can not be directly affected by \( f(t) \) and \( b_i = 1 \) represents an infrastructure vulnerable to the direct application of \( f(t) \).

The dynamic IIM model can be reformulated as follows

\[ \dot{q}(t) = K(A^* - I)q(t) + K B f(t). \]  

In the following remark, we argue that being controllable is a source of vulnerability for the IIM system in Equation (13).

**Remark 1** If the pair \((K(A^* - I), KB)\) is controllable, then all the infrastructures can be made completely inoperable in finite time, i.e., for any \( T > 0 \) there is a choice of \( f(t) \) for all \( t \in [0,T] \) such that \( q(T) = 1 \).

A consequence of the above Remark is that, for a given choice of \( B \) representing one or more concurrent failures or attacks, the fact that the pair \((K(A^* - I), KB)\) is not controllable implies that some infrastructures/sectors (actually, a subspace of the state of the overall state space) can not be made inoperable no matter the magnitude of such combined failures. Hence, we point out that lack of controllability is strongly related with the resilience of the IIM model.

Notice that, when the system is controllable, there are, in general, no hints on the exact shape of \( c^*(t) \) that yields complete inoperability. There is, however, an although theoretical way for an attacker to obtain the complete inoperability of all the infrastructures/sectors in “zero time”, as outlined in the next proposition.

**Proposition 1** Let \( \delta(t) \) be a Dirac pulse and let \( \delta^{(m)}(t) \) be the \( m \)-th derivative of \( \delta(t) \). Let an IIM system having the form of Equation (13) and suppose that \( B \) is a column, i.e., that there is just one input. Moreover, let \( R \) be the controllability matrix of the pair \((K(A^* - I), KB)\) and suppose that the system in Equation (13) is controllable. Then, the initial condition of the system can be forced to \( 1_n \) (complete inoperability) by choosing

\[ f(t) = g_1\delta(t) + g_2\delta^{(1)}(t) + \cdots + g_n\delta^{(n-1)}(t), \]  

where
\[ [g_1, \ldots, g_n]^T = g = R^{-1}1_n, \]  

\textbf{Proof 1} It is well known (see for instance [27]) that, with this choice of \( f(t) \), the initial condition is given by \( q(0) = Rg \). Since the system is controllable, \( R \) is invertible and the statement is proved.

The above result implies that an attack on a single infrastructure can force the inoperability of all the infrastructures to 1 in “zero time”; clearly, such an abstraction is not feasible in practice, but represents an intuitive justification of the following vulnerability metric.

\textbf{Remark 2} Based on Equation (15) we argue that the effort necessary to generate the signal attack \( f(t) \) depends on the magnitude of \( g \). Therefore, in the following, we model the magnitude of the failure/attack by \( ||g||_1 \). In this view, considering Equation (15) we observe that it holds

\[ ||g||_1 = ||R^{-1}g||_1 \leq ||R^{-1}||_1||1||_1 = \sqrt{n}||R^{-1}||_1, \]

meaning that \( ||R^{-1}||_1 \) can be regarded as a measure of the attack effort.

Note further that, if \( R^{-1} \) exists, \( ||R^{-1}||_1 \) gives a rough measure of the fragility of the system; indeed when \( ||R^{-1}||_1 \gg 1 \) a large effort is required to cause large damages, while \( ||R^{-1}||_1 \ll 1 \) implies that the complete inoperability can be reached with a small attack effort and the system is highly vulnerable.

The above remark is the foundation for the definition of a novel vulnerability index. Note that in the following definition we adopt \( ||R||_1 \) as a measure that is inversely proportional to the attack effort. Indeed, we point out that \( ||R^{-1}||_1 \) is a well defined index only if there is just one input and the system is controllable, while by considering \( R \) we can extend the index to the case of multiple inputs and not completely controllable systems.

Let us consider a scenario where a subset of infrastructures \( \Phi \subseteq \{1, \ldots, n\} \) is involved in the attack. Considering Equation (13), we express matrix \( B \) as a vector having entries \( b_i \in (0,1] \) if the \( i \)-th infrastructure is in \( \Phi \), and such that \( b_i = 0 \), otherwise. Notice that the exact value of the entry \( b_i \) depends on the degree of robustness of the infrastructure \( i \) with respect to the direct application of the attack signal \( f(t) \).

\textbf{Definition 1 (Fragility Index)} Let us define the Fragility Index \( \nu \) of an infrastructures subset \( \Phi \subseteq \{1, \ldots, n\} \) as follows:

\[ \nu(\Phi) = ||R||_1, \]

where \( R \) is the controllability matrix of the pair \( (K(A^* - I), KB) \) and \( B \) reflects the impact of \( f(t) \) on the infrastructure subset \( \Phi \).

The fragility index \( \nu \), being inversely proportional to the attack/damage effort, can be regarded as a measure of the overall vulnerability of an IIM system with respect to an adverse event or malicious attack affecting a specific infrastructures subset. Indeed, if \( \nu(\Phi) \gg 1 \) the subset \( \Phi \) is a vulnerable subset, instead, if \( \nu(\Phi) \ll 1 \) the subset \( \Phi \) represent a resilient subset of infrastructures.

\textbf{4.1. Defensive strategy}

We now show that the fragility index can be the basis to guide the decision-maker in the protection of the different sectors. In fact, if the sectors are protected in a way such that the coefficients \( b_i \) are replaced by new coefficients \( \tilde{b}_i \), which are inversely proportional to the sector fragility index, then we can impose arbitrarily small fragility index to the resulting system.

\textbf{Theorem 1} Let \( \nu(\{k\}) \) the fragility index of the sector \( k \). Such an index can be reduced to an arbitrarily small value \( \rho \) by setting \( \tilde{b}_k = \rho \nu(\{k\})^{-1} \).

\textbf{Proof 1} For the sake of simplicity let \( A = A^* - I \) and \( K = I \). Let \( e_i \) be the \( i \)-th vector in the canonical basis of \( \mathbb{R}^n \); i.e., \( e_i \) has all entries equal to 0, except the \( i \)-th entry that is equal to 1.
Moreover, let us denote by $\vec{A}$ the entries of the matrix $\hat{A}$. Let $\Phi = \{k\}$, and consider the associated fragility index $v(k) = \frac{1}{\|\hat{A}_{ik}\|_1}$, where $v(k) = \|e \hat{A} - \vec{A}^n_ik\|_1$. Since $v(k) = \|R\|_1$, it holds $v(k) = 1 + \|e \hat{A} - \vec{A}^n_ik\|_1$.

Let us now adopt a defensive strategy by choosing:

$$\vec{b}_k = \rho v(k)^{-1};$$

the new fragility index $\vec{b}(k)$ is given by

$$\vec{b}(k) = \|\rho v(k)\|_1 e \hat{A} - \vec{A}^n_ik\|_1.$$ 

At this point, plugging Equation (18) in the above Equation we have that it holds

$$\vec{b}(k) = \rho v(k)^{-1} v(k) = \rho.$$ 

This completes our proof. 

The following result is a rather obvious consequence of the above theorem.

**Corollary 1** Let $\rho = [\rho_1, ..., \rho_n]^T \in \mathbb{R}^n$ the column vector whose entries are the new desired fragility indices. We can obtain the desired values by applying the following defensive strategy:

$$\vec{b} = [\rho_1 v(1)^{-1}, ..., \rho_n v(n)^{-1}]^T.$$ 

5. Case study

With the aim to validate the effectiveness of the proposed Fragility Index and its use as a base for the implementation of a defensive strategy, in this section, we propose an experimental analysis with respect to a real world case study.

5.1. Data set

We consider the $15 \times 15$ sector case study in [20, 28, 29] from the 2005 BEA annual IO tables [30].

5.2. Analysis of the proposed index

The upper plot in Figure 1 shows the value of the fragility index $v_i$ by considering infrastructure sets $\Phi$ with cardinality one, i.e., by inspecting the effect of an attack/damage directly affecting one infrastructure at the time. Note that, for the sake of simplicity, we assume $K = 1$ and $b_i = 1$ if the i-th infrastructure is directly involved in the attack. We observe that, in this case, we obtain $v(\Phi) > 1$ for all infrastructures, and the proposed index ranges from about $v(\{1\}) \approx 1.62$ for Agriculture, to about $v(\{3\}) \approx 6.46$ for the Utilities sector. This suggests that a perturbation having the structure of the one discussed in Proposition 1 is amplified from 1.62 to 6.46 times, depending on the affected sector.

The lower plot in Figure 1 shows a comparison among the indices $v_i$ (blue bars), the dependency indices $\delta_i$ (yellow bars) and the influence gains $\gamma_i$ (grey bars) for each infrastructure, normalized with respect to the average. According to the plot, sectors 1 and 2 correspond to a dependency index $\delta_i$ which is significantly above the average, while sectors $3, 5, 8, 9, 11$ are slightly above the average. As for the influence gain $\gamma_i$, we have that sector 5 has a remarkably high value with respect to the average, while sectors $10, 11, 15$ are slightly above the average.

According to Hirschmann [26], therefore, sectors 5 and 11 can be regarded as critical. The results for the controllability index show that sectors $\{3, 4, 5, 7, 12, 13, 14, 15\}$ are above the average, and such a ratio ranges from about 1.03 times the average (sectors 13) to about 1.83 times (sector 3). Such results highlight that the proposed controllability index $v_i$ is able to capture different, possibly complementary, aspects with respect to previous indices. Indeed, while $\delta_i$ and $\gamma_i$ model the...
direct effect of the inoperability of the infrastructures in the short term, the proposed index models the overall effect of the attack/failure, with a larger time scale.

Figure 1. Vulnerability Metrics for 2005 US Infrastructure Sectors case study.

*On top:* Distribution of Fragility Indices $\nu$ for each sector

*On bottom:* Comparison of the indices $\nu$ (dark blue bars), dependency indices $\delta$ (yellow bars), and influence gains $\gamma$ (grey bars). Each index is normalized with respect to the average of its distribution

Figure 2. Fragility indices and controllability matrix rank for multiple attack and resilience coefficients combinations.

*On left:* Average value and variance of the Fragility Index $\nu$ considering multiple attacks ($\text{card}(\Phi) > 1$) and multiple resilience values $b_i$

*On right:* Average value and variance of matrix $R$ considering multiple attacks ($\text{card}(\Phi) > 1$) and multiple resilience values $b_i$

Figure 2 provides additional insights on the proposed metric. Specifically, in Figure 2(left) we report the fragility index $\nu(\Phi)$ for attacks affecting multiple sectors. In the figure, the average value and the variance of $\nu(\Phi)$ are shown considering multiple attack plans $\Phi$ with different cardinality. For each fixed cardinality in the range $[1, \ldots, 10]$, the results in terms of mean value and variance are computed considering all the existing combination of attacks against the considered sectors. Moreover the same results are shown also considering different values of $b_i \in \{0.2, 0.4, 0.6, 0.8, 1\}$ in order to model the effect of the attack depending on the robustness/resilience of the sector or infrastructure being attacked. As an example, for $\Phi = \{2,4\}$ and $b_i = 0.2$ the associated $B$ matrix is defined as $B = [0, 0.2, 0.2, 0.2, 0.2, \ldots, 0]^{T}$. 
The results in Figure 2 (left) highlight that, for each choice of $b_i$, the fragility index increases with increasing number of sectors involved in the attack. Moreover, the effectiveness of the proposed metric in describing the effect of the attack is supported by the increment of fragility index for high values of $b_i$; in fact, high values of $b_i$ represent the fact that the $i$-th sector or infrastructure is prone to the attack. In the same plot when an high resilience level is considered (i.e. $b_i = 0.2$) the fragility index is reduced to low levels. In Figure 2 (right) the rank of the controllability matrix is reported in terms of average value and variance by varying the number of sectors involved in the attack $|\Phi|$ and their resilience $b_i$. The results shown that for each pair of parameters $\Phi$ and $b_i$ the rank of the controllability matrix is always in the range $[11 ... 12]$.

5.3. Defense strategy based on Fragility Index

The following simulation campaign is analysed in order to prove the utility of the defensive strategy based on the fragility indices as explained by Theorem 1. In more details, starting from the same scenario analysed in Figure 1, we adopt a defensive strategy by setting the entries of the new matrix $\tilde{b}$ selecting

$$\tilde{b} = 0.5[v(1)^{-1} \ldots v(n)^{-1}],$$

(22)

where $v(1), \ldots, v(n)$ are the fragility indices collected in the bar plot in Figure 1(top). As highlighted in Figure 3 the new fragility indices $\tilde{v}$ are all equals to 0.5. On the other side, the utility of this kind of defensive strategy is not highlighted by the two other metrics (dependency index, influence gain) because they are based only on the entries of the matrix $A^*$ without considering the resilience coefficients $b_i$.

![Figure 3](image)

**Figure 3.** Comparison of the indices $\tilde{v}$ (dark blue bars), dependency indices $\delta$ (yellow bars), and influence gains $\gamma$ (green bars) in case of defensive strategy. Each index is normalized with respect to the average of its distribution.

6. Conclusions

In this paper we provide a novel metric to evaluate the fragility of a subset of interconnected systems (infrastructures or economic sectors). With respect to the state of the art the proposed fragility index takes into account both the interdependencies and the reactions of each component to an external attack. Hence, it is able to catch the effects of cascade faults or attack by providing an accurate estimation about the fragility of the system. Moreover, we prove the effectiveness of the proposed index as a basis for a defensive strategy against external unpredicted malicious input. Future works will aim at comparing the proposed index with other structural vulnerability metrics, and at analyzing the relation between the fragility index and sector specific vulnerabilities metrics.

7. References

[1] Pasqualetti F, Zampieri S, and Bullo F 2014 Controllability metrics, limitations and algorithms for complex networks *IEEE Transactions on Control of Network Systems* vol. 1, no. 1, pp. 40–52.
[2] Wu-Yan E, Betzel R F, Tang E, Gu S, Pasqualetti F and Bassett D S 2017 Benchmarking measures of network controllability on canonical graph models *arXiv preprint* arXiv:1706.05117.
[3] Summers T H, Cortesi F L and Lygeros J 2016 On submodularity and controllability in complex dynamical networks *IEEE Transactions on Control of Network Systems* vol. 3, no.1, pp. 91-101.
[4] Cam H 2014 Controllability and Observability of Risk and Resilience in Cyber-Physical Cloud Systems *Secure Cloud Computing* pp. 325–343, Springer New York.
[5] Lu Z and Li X 2016 Attack Vulnerability of Network Controllability PloS one vol. 11, no. 9 e0162289.

[6] Solé R V, Rosas-Casals M, Corominas-Murtra B and Valverde S 2008 Robustness of the European power grids under intentional attack Physical Review E vol. 77, no. 2, 026102.

[7] Faramondi L, Oliva G, Pascucci F, Panzieri S and Setola R 2016 Critical node detection based on attacker preferences Proceedings of the 24th Mediterranean Conference on Control and Automation (MED) pp. 773-778.

[8] Faramondi L, Oliva G, Setola R, Pascucci F, Amideo A E and Scaparra M P 2017 Performance Analysis of Single and Multi-objective Approaches for the Critical Node Detection Problem Proceedings of the International Conference on Optimization and Decision Science pp. 315-324.

[9] Faramondi L, Setola R, Panzieri S, Pascucci F and Oliva G Finding Critical Elements in Infrastructure Networks International Journal of Critical Infrastructure Protection.

[10] Faramondi L, Oliva G, Panzieri S, Pascucci F, Schlüeter M, Munetomo M and Setola R Submitted Network Structural Vulnerability: A Multi-Objective Attacker Perspective IEEE Transactions on Systems, Man, and Cybernetics: Systems.

[11] Holme P, Kim B J, Yoon C N and Han S K 2002 Attack vulnerability of complex networks Physical review E vol. 65, no. 5, 056109.

[12] Liu Y Y, Slotine J J and Barabási A L 2011 Controllability of complex networks Nature vol. 473(7346), pp. 167-173.

[13] Liu X, Peng H and Gao J 2015 Vulnerability and controllability of networks of networks Chaos, Solitons & Fractals vol. 80, pp. 125-138.

[14] Haimes Y, Horowitz B, Lambert J, Santos J, Lian C and Crowther K 2005 Inoperability input-output model for interdependent infrastructure sectors I: Theory and methodology Journal of Infrastructure Systems vol. 11, no. 2, pp. 67–79.

[15] Haimes Y and Jiang P 2001 Leontief-based model of risk in complex interconnected infrastructures Journal of Infrastructure Systems vol. 7, no. 1, pp. 1–12.

[16] Santos J R and Haimes Y Y 2004 Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures Risk Analysis vol. 24, pp. 1437–1451.

[17] Kalman R E 1963 Mathematical description of linear dynamical systems Journal of the Society for Industrial & Applied Mathematics, Series A: Control vol. 1, no. 2, pp. 152–192.

[18] Leontief W W 1966 Input-Output Economics, Oxford University Press.

[19] Miller E M and Blair P D 2009 Input-Output Analysis: Foundations and Extensions 2nd ed., Cambridge University Press.

[20] Barker K and Rocco C M 2011 Evaluating uncertainty in risk-based interdependency modeling with interval arithmetic Economic Systems Research vol. 23, no. 2, pp. 213–232.

[21] Oliva G, Panzieri S and Setola R 2011 Fuzzy dynamic input-output inoperability model International Journal on Critical Infrastructure Protection vol. 4, no. 3–4, pp. 165–175.

[22] Setola R 2010 How to measure the degree of interdependencies among critical infrastructures Int. J. of System of Systems Engineering vol. 2, no. 1, pp. 38–59.

[23] Setola R, De Porcellinis S, and Sforna M 2009 Critical infrastructure dependency assessment using the input-output inoperability model International Journal of Critical Infrastructure Protection vol. 2, no. 4, pp. 170–178.

[24] Chenery H B and Watanabe T 1958 International comparisons of the structure of production Econometrica vol. 26, no. 4, pp. 98–139.

[25] Rasmussen P 1956 Studies in Intersectorial Relations, North Holland, 1956.

[26] Hirschmann A O 1958 The Strategy of Economic Development, Yale University Press.

[27] Kailath T 1980 Linear systems. vol. I Englewood Cliffs, NJ: Prentice-Hall.
[28] Barker K and Haimes Y Y 2009 Uncertainty analysis of interdependencies in dynamic infrastructure recovery: Applications in risk-based decisionmaking *Journal of Infrastructure Systems* vol. 15, n. 4, pp. 394–405.

[29] Oliva G, Setola R and Barker K 2014 Fuzzy Importance Measures for Ranking Key Interdependent Sectors Under Uncertainty *IEEE Transactions on Reliability* vol. 63, n. 1, p. 42–57.

[30] Bureau of Economic Analysis 2007 *Input-Output Accounts Data* [http://www.bea.gov](http://www.bea.gov).