SAND2020-3057C

A Complex Systems Approach to Develop a Multilayer Network Model for High Consequence Facility Security

Adam D. Williams, Gabriel C. Birch, Thushara Gunda, Sue Caskey, Thomas Adams, Jamie Wingo
Sandia National Laboratories[1], Albuquerque, NM, USA, [adwilli; gcbirch; sacaske; tgunda]@sandia.gov

ABSTRACT (315/500 words)

Protecting high consequence facilities (HCF) from malicious attacks is challenged by the increasing complexity observed in today's operational environments and threat domains. This complexity is driven by a multi-faceted—and interdependent—set of trends that include the analytical challenge of modeling the intentionality of adversaries, (r)evolutionary changes in adversary capabilities, and less control over HCF operating environments. Current HCF security approaches provide a strong legacy on which to explore next generation approaches—including recent calls to more explicitly incorporate multidomain interactions observed in HCF security operations. Insights from complex systems theory and advances in network science suggest that such interactions—which can include relationships between adversary mitigation mechanisms (e.g., physical security systems and cybersecurity architectures) and facility personnel and security procedures—can be modeled as interactions between layers of activities. From observation and qualitative data elicited from diverse HCF security-related professionals, applying such a "layer-based" approach is a promising solution for capturing the interdependencies, dynamism, and non-linearity that challenge current approaches. Invoking a multilayer modeling approach for HCF security leverages network-based performance measures which (1) helps shift underlying design, implementation, evaluation, and inspection from a "reactive" to a "proactive" ethos; (2) incorporates multidomain interactions observed in HCF security; and, (3) builds a better foundation for exploring HCF security dynamics and resilience.

After exploring these interactions between cyber, physical, and human elements—this paper introduces major modifications to conceptualizing HCF security grounded in data elicited from a range of related subject matter experts. Next, this paper leverages insights from the systems theory and network science literatures to describe a method of constructing complex, interdependent architectures as multilayer directed networks to better describe HCF security. The utility of such a multilayer network-based approach for HCF is security is then demonstrated with a hypothetical example. Lastly, key insights are summarized and the implications of incorporating network analytical performance measures into HCF are discussed.

INTRODUCTION

According to the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security, critical infrastructure are those assets, systems, or networks whose incapacitation or destruction would have a debilitating effect on national security, economic prosperity, or public health/safety [1]. Similarly, CISA identifies several sectors of critical infrastructure that consists of "high consequence facilities (HCF)" whose benefits are tied to materials, processes, or systems that pose unique risks, including the chemical, energy, and the nuclear reactors, materials, and waste sectors. Protecting HCFs from malicious attacks is challenged by increasing complexity observed in today's operational environments and threat domains.

[1] SAND2020-XXXX. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

This complexity is driven by a multi-faceted—and interdependent—set of trends. The first is the analytical challenge of modeling the intentionality of possible adversary actions, which can range from unwitting or accidental (almost random) acts to actions tailored to optimize chances of successfully completing a malicious act. Second, potential adversaries are demonstrating both evolutionary and revolutionary-type improvements in their resources, capabilities, and tactics. Consider the use of advanced unmanned aerial systems by Yemeni rebels to attack Saudi Arabian oil facilities in September 2019 [2], the cyber-attack on the Kudankulam nuclear power plant in India in October 2019 [3], and a 2011 DHS memo stating that "violent extremists have, in fact, obtained insider positions" for damaging physical and cyber-attacks [4] as representative examples. Third, the operating environment in which HCFs must exist is changing, including increased digitization [5], interdependency [6], and operations in non-traditional (e.g., remote) locations [7]. Whether considered individually or taken together, these changes reduce levels of control over the operational environments—which has been a long-standing pillar of security for HCFs. Thus, there is a need to better incorporate elements of operating environments into HCF security [8]. Lastly, as these challenges engender more stringent and comprehensive security responses, levels of organizational (and individual) inertia grow as such changes are seen as opposing normal workplace activities. Thus, in addition to a more complete understanding of threats facing HCFs, there is an additional need to better understand how organizational and human influences impact HCF security performance [9].

Current approaches to HCF security are primarily based on a solution developed by Sandia National Laboratories (Sandia) in the late 1970s and early 1980s. This approach, called, the *Design Evaluation Process Outline* (DEPO), was a response to a 1973 Congressional mandate to improve the security of nuclear materials [10]. Borrowing from the success of probabilistic risk assessment in nuclear safety, DEPO calculates the ability of a collection of security components to achieve a defined probability of defeating a specific adversary along a specific attack path [11] [12]. This methodology defines system effectiveness as the product of the conditional probability that detection and delay system components assess an adversary in time for response forces to arrive onsite to engage (e.g., the probability of interruption) and the conditional probability that, upon arriving, the response force can kill, capture or cause the adversary to flee (e.g., the probability of neutralization). DEPO uses this *detect, delay, respond* paradigm to fully describe the necessary functions of HCF security.

Yet, DEPO and its derivatives struggle to account for the previously discussed set of challenges to HCF security. At the same time, DEPO provides a strong legacy on which to explore next generation HCF security approaches. Previous arguments [13] have made the case for exploring he multidomain interactions often observed in HCF security operations in terms of complex system behaviors and models for HCF security. Such interactions include, but are not limited to, the relationships between adversary mitigation mechanisms (e.g., physical security systems and cybersecurity architectures); facility personnel and security procedures; security mechanisms and facility infrastructure; or enhanced adversary capabilities and HCF security upgrades.

MULTIDOMAIN INTERACTIONS IN HCF SECURITY

To further understand these challenges to HCF security, interviews and focus groups with subject matter experts (SMEs) were conducted to capture the dynamics and perceptions underlying these interactions in HCF security. Using a semi-structured approach, pre-determined, open-ended questions were used to elicit more coherence, depth and density with which to understand and unpack interviewee responses [14]. This qualitative data collection probed perceptions of the current state of security assessments; strengths and weaknesses of current HCF-related security approaches; and, depictions of ideal future states for HCF security. These interviews and focus groups

(summarized in Table 1)—with participants from a diverse set of HCF security-related backgrounds—provided data for describing and better understanding the interactions and dynamics that need to be captured in next generation HCF security approaches.

Table 1. Summary description of interviews and focus groups with HCF security professionals.

Int.	HCF Security-Related Role	Training in Current HCF Approaches	Years Involved in HCF Security-Related Role(s)*	Formal Analytic Background
A	1	Formal	>10	No
B	1	Formal	>10	No
C	2	Informal	>2	Yes
D	1	Informal	>10	No
E	3	--	>6	Yes
F	4	Formal	>2	Yes
G	5	Informal	>5	No
H	5	Formal	>10	No
I	3, 4	--	>5	Yes
J	4	--	>10	Yes
K	1	Formal	>20	No
L	5	--	>10	No
M	4, 6	Formal	>30	Yes
N	7	--	>10	Yes
O	4, 6	Informal	>30	No
P	3, 4	Formal	>15	Yes
Q	1, 4	Informal	>5	Yes
Focus Group 1	6	Informal	2 to 30+	Some
Focus Group 2	1, 5	Informal	0.5 to 7	No

1. *HCF Security Engineering*; 2. *Cyber Security Analysis*; 3. *HCF Resilience Analysis*; 4. *HCF Security System Analysis*; 5. *HCF Security Technology Development*; 6. *HCF Security Operations*; 7. *Human Cognition in HCF Security*

*This refers to ***cumulative*** years in HCF security-related roles, not just the current role

Analysis of this qualitative data relied "less on counting and correlating and more on interpretation, summary and integration" [14, p. 3]. Evaluation focused primarily on finding themes in the data and identifying insightful outlier comments germane to better understanding how multidomain interactions impact HCF security. For example, though most of our interviewees supported our research goal, one outlier comment came from Interviewee Q who strongly expressed that it was time to move past current HCF analytical paradigms that are "static and dated."

One theme that emerged was the current *siloed nature* of HCF security-related activities. The data identified limited (if existing) interactions between security and facility personnel, security designers and implementers, and different domain security personnel (e.g., physical vs. cyber), crystallized by Interviewee P who said "stovepipes kill us." The data also suggests that bridging these siloes extends beyond technical alignment and includes overcoming challenges related to different cultures among different perspectives of HCF. In response was the consensus that a systems approach could help bridge some of these siloes by clarifying specific role(s) and objective(s) for each perspective (e.g., security operations personnel focus on ensuring power supply vs. cyber security personnel focus on preventing hackers) and illustrating how these role(s) work together to achieve HCF security.

A second theme from the data related to the inadequate consideration of the role of human actors in HCF security. Whether a need to better address complacency in security personnel, overcoming the

"prevalence effect" [15], better understanding impacts from nuisance/false alarm rates, or mitigating insider threats, our data suggests the role of human actors needs to be better understood and more explicitly accounted for in HCF security approaches. For example, Interviewee Q discussed an anecdote relating to HCF security that concluded with the sentiment that having the best security system is still not beneficial if the human elements within the system do not use or access the information provided by technological elements.

A third theme from our data is the impact of the incomplete characterization of HCF-related threats. For example, Interviewee D described this occurs because the HCF security community has to "see it to believe it," while Interviewee P depicted a prevailing attitude of "what's happening overseas could not possibly happen in the U.S." Rather than relying on purely quantitative descriptions of threats (like the popular *design basis threat* [11]), our interview data identified benefits in a threat-agnostic paradigm that would improve HCF security capabilities for responding to various emerging—including un-anticipatable—future threats. Such a paradigmatic shift moves the HCF security design objective, according to one interviewee, from identifying "what is the probability of adversary success" to "influenc[ing] the attacker's deterrence" (Interviewee P).

Evaluation of our interview and focus group data highlighted the need for HCF security solutions to not only meet desired security objectives, but also to consider the impact on overall HCF safety and operations. Across our data, there was a positive response to the goals of this research to more formally identify and incorporate multidomain interactions into HCF security analysis. Moreover, our interviewees further supported taking a systems approach to HCF security and recasting traditional thinking on security performance in broader, more interdependent terms to describe HCF security system stability and adaptiveness in an emerging environment.

MULTILAYER NETWORK MODEL FOR HCF SECURITY

Leveraging insights from the complex systems and network theory domains provides potential pathways for closing the gaps identified in our data and current best practices for HCF security. From a complex systems theory perspective, linear concepts of cause and effect are replaced with a non-linear understanding of cause and effect as parallel processes because "meaning is achieved through connections" [16, p. 4]. Yet, these many, simple interacting components can produce performance different from what would be expected from individual components. This suggests an opportunity to identify more dynamic performance measures better able to describe the efficacy and effectiveness of HCF security amidst previously described challenges.

Building on the argument that relationships (or, interactions) can characterize relative priority between nodes (or, system components) to describe emergent behaviors [16], network theory provides additional insights useful to overcome current challenges to HCF security [17]. There has long been a link between network theory and complex systems [18], but more recent efforts (e.g., [19] and [20]) are investigating the impacts of multiple, interacting layers within a single network. For example, applying traditional network theoretic approaches to multiple layers provides performance measures such as multilink community detection, versatility, and multilayer communicability [21] that capture complex characteristics underlying HCF security system design.

This breadth of performance measures effectively expands the definition of HCF security and moves closer to meeting the calls for "threat-agnostic" approaches highlighted in the interview and focus group data. From an analytical perspective, shifting toward threat agnosticism provides greater flexibility in responding to revolutionary changes in security threats than traditional approaches that

are tied to smaller, evolutionary threat changes captures in the design basis threat. For example, *multilayer communicability*—defined as "a centrality measure which quantifies the number of paths taking both intralinks and interlinks that join a given node of a given layer to the other nodes of the multilayer structure" in [21]—helps describe the potential for digital manipulations to cascade through other domains of HCF security performance. As implied by this example, a multilayer network-based approach also helps take advantage of a larger portion of generated data and better positions HCF security analysis to incorporate dynamic measures of performance.

Coordinating these rich insights lays the foundation for describing the multi-domain interdependencies necessary to align next-generation HCF security capabilities with current dynamic trends. From experience, observation, and confirmed by our data, applying such a "layer-based" approach is a promising solution for capturing the interdependencies, dynamism, and non-linearity that challenges current approaches. In earlier work [13], these layers were described in terms of traditional HCF terms, namely: physical protection systems, cybersecurity architectures, human/organizational actors, and facility infrastructure. (It is of note, however, that these latter two layers—let alone their interactions with the former two—receive minimal consideration in current approaches.) In this work, we propose a *function-based* layer framework that enables capturing various functional capabilities within the HCF and framing them in a manner enabling the calculation and evaluation of related interactions using network analysis techniques.

A representative set of notional layers to describe HCF security include:

- **Layer 1-Physical:** Consisting primarily of the *physical* components that compose a HCF security system, it traditionally includes technologies to support detection (e.g., sensors), delay (e.g., building surfaces), and response functions (e.g., HCF security personnel) that are selected to increase the time or resources necessary to complete a malicious act.
- **Layer 2- Data and Communications:** Consisting primarily of the components that support *data* flows for HCF security, these components are modeled as data *generators* (which collect or manipulate data, like exterior microwave sensors) and data *receivers* (which typically process, store, and display information to human operators, like CCDE monitors).
- **Layer 3-Supporting Infrastructure:** Though often overlooked in traditional approaches, strong HCF security is dependent on a physical infrastructure components that act as an underlying skeleton to provide the necessary operating conditions (e.g., adequate power, temperature control, or fluid flow) for other nodes (and layers).
- **Layer 4-Human Actor(s):** Perhaps most challenging, this layer is intended to more explicitly describe the role(s) of human in meeting HCF security operations. While the "nodes" in this layer consist of human actors, the structure of this layer helps describe their relative impact in terms of connectedness between nodes.

DEMONSTRATION CASE: HCF SECURITY SCENARIOS

A hypothetical high consequence facility (H^2CF) security system was generated to explore the effectiveness and efficacy of a multilayer network representation of the components and relationships described in the previous section. A modified version of the hypothetical facility used in [13], this H^2CF security system is composed of five distinct perimeter intrusion detection zones (i.e., sectors). Figure 1—developed with the MuxViz tool described in [22]—shows the multilayer representation of this five-sector perimeter intrusion detection system. Following HCF security best practices (e.g., [12]), each sector contains sensor devices and cameras that capture data from their

areas of responsibility. In addition, these sensors and cameras are connected to junction boxes that exist within the physical layer and serve as aggregating points within each sector for communication and power. All related sensor and video data is directed towards the command control display systems (CCDE), which acts as the primary human interface to determine the state of the H^{2}CF security system.

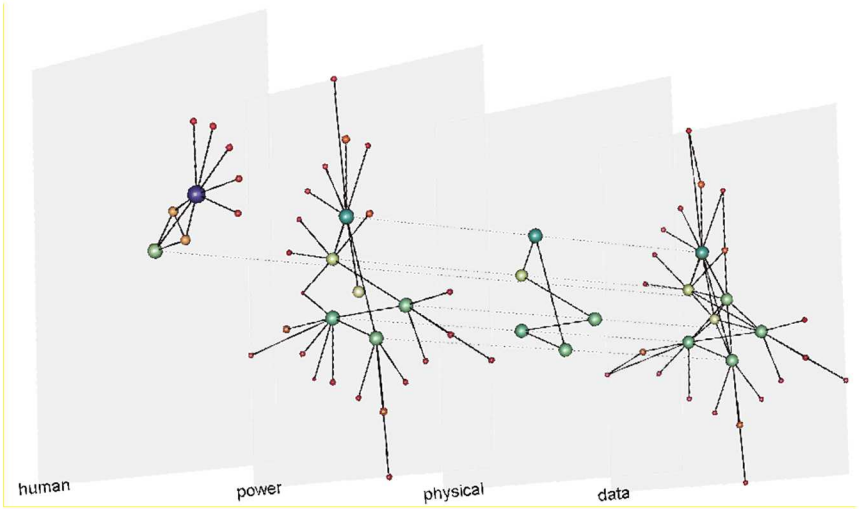

Figure 1. Example multilayer representation of a five-sector hypothetical high consequence facility, where the PageRank algorithm was used to determine node size and color (where, larger/bluer nodes have higher PageRank values and smaller/redder nodes have lower PageRank values).

For the multilayer model of the H^{2}CF in Figure 1, nodes in the data layer consist of twenty data generators (e.g., ten sensors, five cameras, five algorithmic processors, etc.), five data transfer elements (e.g., network switches), and two data aggregators (e.g., the CCDE and video management system (VMS)). For clarity, the physical infrastructure layer solely consists of a representation of five junction boxes—one for each security sector—which aggregate security-related information and data across multiple layers. This representative H^{2}CF security system embeds redundancy in both the communication and power layers. For example, junction boxes (nodes within the physical layer shown in Figure 1), are connected in a ring configuration. Such a design ensures that both communication and power continually operate even when one link is broken. Similarly, the supporting infrastructure layer focuses on power generation and delivery. A backup power supply is connected to the network, adding an additional redundant power connection if a connection to the larger power grid is severed. These elements are shown within the power layer. Lastly, the human layer illustrates organizational relationships between human actors in the H^{2}CF—including the CCDE operator, HCF security supervisor, HCF security officers, and HCF response forces.

The PageRank algorithm was performed on this multilayer network (Figure 1) to consider both intra- and inter-layer links between nodes. Note, larger/bluer nodes represent higher PageRank values and smaller/redder nodes represent lower PageRank values. For example, analysis of this representative five-sector H^{2}CF suggested that that the human security commander (the large purple node in the "human" layer in Figure 1) was the highest ranked element within the multilayer system.

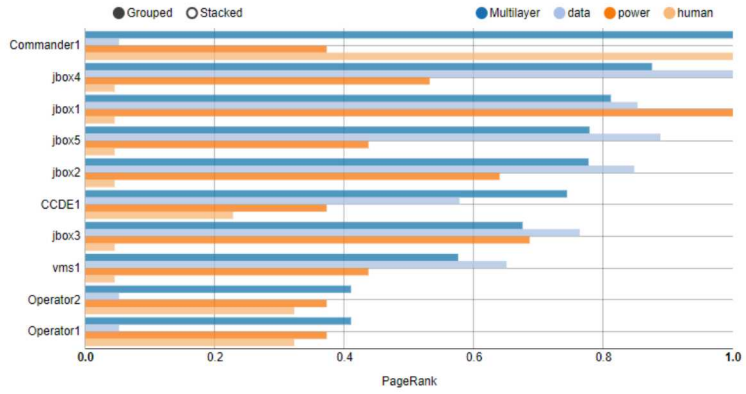

Figure 2. Ten highest PageRank values for the five-sector H^{2}CF shown in Figure 1.

Figure 2. shows the ten highest PageRank nodes within the system across the different H^{2}CF layers. Preliminary analysis indicates that, while the human commander may be most critical, junction boxes also play vital roles—stemming from their collection and distribution of power and information across the layers to other elements at the edges of the network. Elements such as the CCDE and VMS also play critical roles, but interestingly have lower PageRank values than most junction boxes. Surprisingly, human operators had the two lowest PageRank value for this H^{2}CF network.

INSIGHTS & IMPLICATIONS

Constructing a multilayer model-based approach enabled investigation of traditionally qualitative insights and design best practices for HCF security in a more quantitative manner. The PageRank algorithm indicated that two commonly identified elements in an HCF, the human commander and the central data aggregating points, were of high importance. This maps closely to qualitative insights held by traditional HCF security approaches, such as the previously described DEPO method. However, this analysis quantitatively identified the critical nature of the junction box elements within the H^{2}CF. These insights could point towards new strategies to decentralize, protect, or optimize subcomponents within the HCF for a more balanced distribution of importance within the network.

The themes and insights from the data set supported this approach to security and helped establish the conceptual translation between network-based performance measures and HCF security behaviors. For example, the ability to calculate quantitative network-metric comparisons—based on PageRank in this preliminary analysis—of components in an HCF enable analyses and evaluations that move away from a prescribed threat-based evaluation towards a threat-agnostic, holistic system architecture perspective. Modeling HCF as multilayer systems with many interdependent components enables capturing relational impacts between traditionally segregated domains of security design (e.g., cyber, physical) and results in deeper insights into HCF security behaviors.

These insights imply the potential to expand the multilayer network representation from a static system and move towards dynamic representation. This would enable the calculation of network metrics and analyses that capture the interactivity found within HCF security architectures. Evolving this modeling capability to look at HCF security would shift underlying design, implementation, evaluation, and inspection perspectives from a "reactive" to a "proactive" ethos. Further study and development is needed to adequately incorporate such dynamism and resilience. Yet, this multilayer network model provides a strong start to better address the role(s) of human actors, multidomain interactions, and non-linear operational environments that impact HCF security performance against real-world complexities, innovative adversaries, and disruptive technologies.

REFERENCES

[1] Cyber Infrastructure Security Agency, U.S. Department of Homeland Security, "Critical Infrastructure Sectors," 4 March 2020. [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors.

[2] B. Hubbard, P. Karasz and S. Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran," The New York Times, 19 September 2013. [Online]. Available: https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html. [Accessed 4 March 2020].

[3] A. Campbell and V. Singh, "Lessons from the cyberattack on India's largest nuclear power plant," Bulletin of the Atomic Scientists, 14 November 2019. [Online]. Available: https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/. [Accessed 4 March 2020].

[4] Homeland Security News Wire, "DHS warns utilities at risk from insider threats," 25 July 2011. [Online]. Available: http://www.homelandsecuritynewswire.com/dhs-warns-utilities-risk-insider-threats. [Accessed 4 March 2020].

[5] A. V. Gheorge and M. Schlapfer, "Ubiquity of digitization and risks of interdependent critical infrastructures," *IEEE International Conference on Systems, Man, and Cybernetics,* vol. 1, pp. 580-584, 2006.

[6] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine,* no. 6, pp. 11-25, 2001.

[7] U.S. Department of Homeland Security, "The Power of Testing Critical Infrastructure in Operational Settings," 19 November 2018. [Online]. Available: https://www.dhs.gov/science-and-technology/blog/2018/11/19/power-testing-critical-infrastructure-operational-settings#. [Accessed 4 March 2020].

[8] A. D. Williams, "The Importance of Context in Advanced Systems Engineering," in *Systems Engineering in the Fourth Industrial Revolution: Big Data, Novel Technologies, and Model Systems Engineering*, Hoboken, NJ, John Wiley & Sons, 2020, pp. 45-75.

[9] A. Williams, "Beyond Gates, Guards, & Guns: The Systems-Theoretic Framework for Nuclear Security," Massachusetts Instistute of Technology, Dissertation, Cambridge, MA, 2018.

[10] W. J. Desmond, N. R. Zack and J. W. Tape, "The First Fifty Years: A Review of the Department of Energy Domestic Safeguards and Security Program," *Journal of Nuclear Materials Management,* vol. 26, no. 2, 1998.

[11] M. L. Garcia, The Design and Evaluation of Physical Protection Systems (2nd Ed.), Butterworth-Heineman, 2008.

[12] B. Biringer and J. Danneels, "Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures," in *Risk-Based Decision Making in Water Resources IX*, Santa Barbara, 2000.

[13] A. D. Williams and G. C. Birch, "A Multiplex Complex Systems Model for Engineering Security Systems," in *IEEE Systems Security Symposium*, Crystal City, VA, In-press.

[14] R. D. Weiss, Learning from Strangers: The Art and Method of Qualitative Interview Studies, New York: The Free Press, 1995.

[15] J. Wolfe, D. Rubinstein and T. Horowitz, "Prevalence effects on newly trained airport checkpoint screeners: Trained observers miss rare targets, too," *Journal of Vision,* vol. 13, no. 3, 2013.

[16] J. Tranquilo, An Introduction to Complex Systems: Making Sense of a Changing World, Switzerland: Springer Nature, 2019.

[17] A. D. Williams and K. A. Jones, "Invoking Network & System Theory to Improve Security Risk Management in International Spent Nuclear Fuel Transportation," in *Proceeedings of the 58th INMM Annual Meeting*, Palm Desert, CA, 2017.

[18] Y. Liu, J. Slotine and A. Barabasi, "Control centrality and hierarchical structure in complex networks," *PLoS One,* vol. 7, no. 9, p. e44459, 2012.

[19] M. Kivela, A. Arenas, M. G. J. Barthelemy, Y. Moreno and M. Porter, "Multilayer Networks," *Journal of Complex Networks,* vol. 2, no. 3, pp. 203-271, 2014.

[20] S. Gomez, J. Diaz-Guilera, C. Gomez-Gardenas, Y. Perez-Vicente, Y. Moreno and A. Arenas, "Diffusion Dynamics on Multiplex Networks," *Physical Review Letters,* vol. 110, no. 2, p. 028701, 2013.

[21] G. Binaconi, Multilayer Networks: Structure and Function, Oxford: Oxford University Press, 2018.

[22] M. De Domenico, M. A. Porter and A. Arenas, "MuxViz: a tool for multilayer analysis and visualization of networks," *Journal of Complex Networks,* vol. 3, no. 12, pp. 159-176, 2015.