A systematic review of cyber-resilience assessment frameworks

Sepúlveda Estay, Daniel Alberto; Sahay, Rishikesh; Barfod, Michael Bruhn; Jensen, Christian D.

Published in:
Computers & Security

Link to article, DOI:
10.1016/j.cose.2020.101996

Publication date:
2020

Document Version
Peer reviewed version

A structured review of cyber-resilience assessment frameworks

Daniel A. Sepúlveda-Estay[1], Rishikesh Sahay[3], Michael B. Barfod[1], and Christian D. Jensen[2]

[1]*Department of Technology, Management and Economics, Technical University of Denmark*

[2]*Department of Applied Mathematics and Computer Science, Technical University of Denmark*

[3]*Man Energy Systems*

December 23, 2019

Abstract

Cyber-attacks are regarded as one of the most serious threats to businesses worldwide. Organizations dependent on Information Technology (IT) derive value not only from preventing cyber-attacks, but also from responding promptly and coherently when cyber-attacks happen so as to minimize their disruptive effect on operations. This capacity is known as cyber-resilience. As multiple cyber-resilience frameworks (CRF) have been proposed, increased clarity about the scope, characteristics, synergies and gaps in existing CRFs will facilitate scientific research advancement in this area. This paper uses a structured literature review to identify extant research on CRFs. This analysis is based on a sample representing 36 different industries and 25 different research areas. Through the use of descriptive analysis, network analysis, text analysis and thematic categorization this paper categorizes CRFs as either strategic or operational, and according to the hierarchy of their decision influence, attacks addressed, the methods used and the places and institutions doing CRF research. As a result, this work presents an overview of the current CRF research landscape, identifies relevant research gaps, highlights similarities and synergies between CRFs, and proposes opportunities for interdisciplinary research, as a contribution to guide future research in this area.

Keywords— Literature Review, Cyber-Resilience

1 Introduction

The increasing dependence of systems on Information Technology (IT) has been fundamental to the management of increasingly complex systems and operations. Online connection supports the operation of critical infrastructure such as smart grids, railways, and healthcare. Additionally, the substantial growth in number of online support services available for these industries simplifies the identification and resolution of operational issues.

However, in light of the recent surge in cyber attacks on these services, such enhanced connectivity has also led to new challenges for maintaining the availability, integrity and confidentiality of these services . The complexity of interconnected systems has led to the unintentional

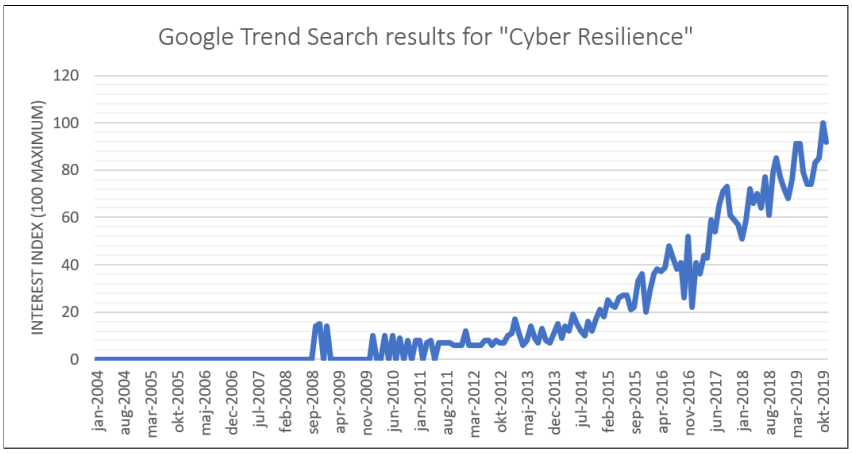

Figure 1: Google search trends about cyber resilience since 2004 [2]

creation of vulnerabilities which expose connected organizations to negative consequences in their physical operations from cyber attacks.

Cyber resilience, the capacity of a system of recovering from the consequences of a cyber-attack, has been identified as a desirable system capability [1], and is a topic that is receiving increasing attention, as can be seen from an analysis of the google search trends shown in Figure 1 [2]. Cyber-resilience has been understood at different levels of aggregation. At a strategic level, cyber-resilience has been first implemented as coverage to disruption-derived losses through insurance. However, such an approach to resilience presents at least four relevant shortcomings. First, insurance only covers financial indemnification and is inherently unable to cover non-financial side effects of a cyber-attack, such as loss of reputation. Second, insurance only covers a specific subset of hazards, while unknown or highly unlikely events either have a very high premium, or are not covered at all. Third, insurance is the transfer of funds without the construction of any capabilities, and as such does not necessarily lead to a lower likelihood of a cyber-attack from happening again. Finally, insurance remains an expense even if no cyber-attack takes place.

Despite efforts to better manage unexpected breakdowns, scientific literature highlights the inadequacy of existing models for understanding and predicting breakdown in complex systems [3], resulting from a lack of tools for designing an adequate system response that will avoid, or limit the consequences of, operational disruption.

This inadequacy is further expanded by the problem of cyber attacks, as breakdowns of interconnected systems can be triggered from anywhere in the world with little to no traceability and perfect reproducibility.

Coherent and efficient future research can be aided greatly by understanding the Cyber Resilience Frameworks (CRFs) that have already been proposed, e.g., the types of attacks these frameworks address, the methods that are used, and the institutes and countries where these CRFs are investigated, for example.

As a result, this research paper uses a reproducible method to gather and synthesise information about the CRFs that have been put forward by the scientific community, to reveal their characteristics by answering questions like:

1. What types of attacks are addressed by CRFs proposed in literature?
2. Which methods do these proposed CRFs use?
3. Which countries and institutions have proposed CRFs?", and
4. Which research and industrial areas do existing CRFs cover?

These answers are expected to contribute to a foundation for understanding the present

SLR parameter	Description
SLR framework	Durach et al., (2017)
Context for research	The recovery to cyber attacks (Cyber-resilience) is a desirable quality of systems. The rapid proposal of cyber-resilience frameworks justifies the effort of summarizing what has been published through a structured, reproducible process.
SLR relevance	The review of extant literature about cyber-resilience frameworks can highlight areas for future research and guide cross-disciplinary research.
Unit of analysis	Published articles in peer-reviewed journals
Research questions	What are the cyber-resilience frameworks published in literature?
Sources of data	Search engine from the international scientific article database Web of Science
Search Strategy	a.- Use search engines with the title keyword combinations to obtain the baseline sample b.- Filter the baseline sample by using the Exclusion criteria 1 & 2 to obtain the synthesis sample.
Title keyword (Search) Combinations	Cyber AND (Resilience OR Resilient OR Resiliency OR Vulnerability OR Attacks OR Disruption OR Recovery OR Framework OR Mitigation)
Exclusion Criteria 1	a.- Only scientific articles b.- Written in English c.- Has an abstract
Exclusion Criteria 2	Title or abstract contains "framework"

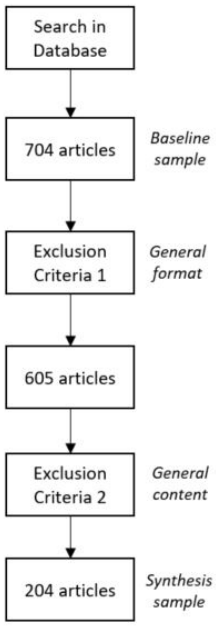

Figure 2: SLR protocol and resulting process

CRF research landscape, aid in the cross-pollination of approaches and ideas between research areas and industries, and to foster networking between CRF research groups.

Section 2 presents the structured literature review methodology (SLR). Section 3 presents the results obtained through a descriptive analysis. Section 4 presents the analysis of the results through text mining and clustering methods. Section 5 presents a thematic analysis of the sample. Finally, section 6 discusses the identified synergies between CRFs and mentions relevant gaps and research opportunities.

2 Methodology

Literature reviews have been documented to be effective sources for creation of knowledge, through the structured gathering of existing scientific work and the use of direct or meta-analysis of explicit or tacit information synthesis, with the aim of answering specific research questions [4].

This paper uses a structured literature review process (SLR) as documented guidelines as outlined by Durach et al [5]. Durach builds on both the frameworks by Murlow [6] for the medical field and its adaption by Tranfield [7] to management, resulting in a method that is appropriate for research across different fields where there might be divergence about what is found important.

The resulting SLR is a comprehensive, explicit and reproducible method for the selection and analysis of scientific publications, to provide evidence for the identification of published CRFs. The SLR protocol is detailed in Figure 2.

Search criteria were applied to specific publication databases in September 2019, results in 704 published articles, the `baseline sample`. These articles were filtered through the use of the `exclusion criteria 1` related to the articles' general format, which narrowed the search down to those articles written in English, not related to scientific conferences, that contain an abstract. This excluded conference paper, book reviews, news articles or editorial notes, for example, from the final analysis. Exclusion criteria 1 gave as a result an article sample set of 605 articles.

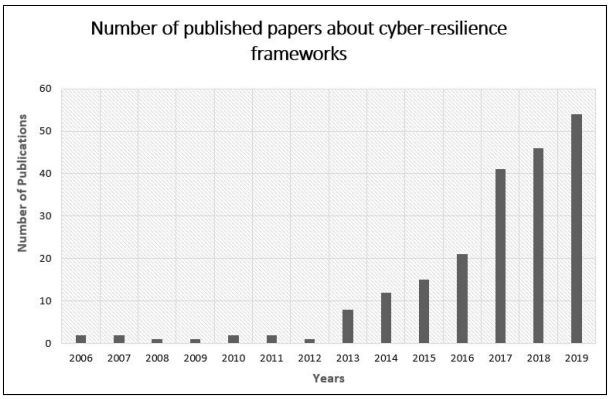

Figure 3: Number of articles published about CRF

This set is narrowed further through the use of `exclusion criteria 2` related to the articles' general content. Articles that did not contain the word `"framework"` either in its title or its abstract, were excluded from the final set. This final set, denominated the `synthesis sample`, contains 208 articles. The `synthesis sample` is analyzed first through a descriptive, then through a text and clustering analysis and finally through a thematic analysis.

3 Descriptive analysis of search results

The `synthesis sample` reflects an exponential increase in the number of articles published about CRFs. This is represented in Figure 3, and this increase is very similar to the increase in google-trend search enquiries shown in Figure 1.

The earliest reference found by our review process of an article proposing a framework to manage cyber-attacks is by a Japanese research group from NEC Corporation in March 2006, related to a framework against virus infections in network systems [8]. This was closely followed the same year by a research group from the University of Virginia which proposed a model to manage the cyber-security of intellectual property [9]. The earliest European publication found in the sample is an article from 2008 by a collaboration between the University of Lund in Sweden, and the University of Portsmouth in England, presenting a framework for the investigation of cyber-crime [10]. The earliest article found about the proposal of a CRF is from 2011, when a collaboration between Carnegie Mellon University and the University of Virginia published research about modeling of cyber-intrusions to cyber-infrastructure in order to increase cyber-resilience [11].

Most journals in our sample have published only one or two articles about CRFs as can be seen in Figure 4. This represents a highly disperse yet diverse publication landscape. A notable exception is the journal *IEEE Transactions on Smart Grid*, with ten publications related to CRF.

An analysis of the number of citations for the papers in the sample shows that a great majority of these do not have a citation, and only very few have a great number of citations, as shown in Figure 5. The article with the most citations in our sample is a paper by Pasqualetti et al., titled *"Attach detection and identification in cyber physical systems"* [12] with 495 citations at the time of extracting the synthesis sample in September 2019, while 64 articles had no citations at that same synthesis sample extraction date.

The authors of these papers are also from diverse nationalities. Authors from 47 different countries were represented in the sample. Figure 6 represents the proportion of the number of collaborating countries found in the synthesis sample papers. Collaboration was determined by the number of distinct countries to which the paper authors have been registered. Over 70% of papers represented in the sample, are the result of single authorship or national col-

Journal	Number of Publications
IEEE TRANSACTIONS ON SMART GRID	10
SENSORS	6
FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE	6
COMPUTERS & SECURITY	5
IEEE SYSTEMS JOURNAL	4
IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS	4
IEEE ACCESS	4
JOURNAL OF DEFENSE MODELING AND SIMULATION-APPLICATIONS METHODOLOGY TECHNOLOGY-JDMS	4
INTERNATIONAL JOURNAL OF CYBER WARFARE AND TERRORISM	4
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION	4
COMPUTERS IN INDUSTRY	3
SECURITY AND COMMUNICATION NETWORKS	3
IEEE TRANSACTIONS ON POWER SYSTEMS	3
IEEE TRANSACTIONS ON AUTOMATIC CONTROL	3
INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS	3
INFORMATION SCIENCES	3
IEEE TRANSACTIONS ON SYSTEMS MAN CYBERNETICS-SYSTEMS	3
OTHER JOURNALS	136
Total number of papers	**208**

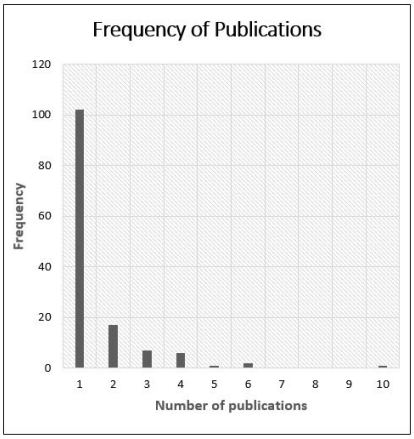

Figure 4: Name and frequency of journals that have published articles about CRF

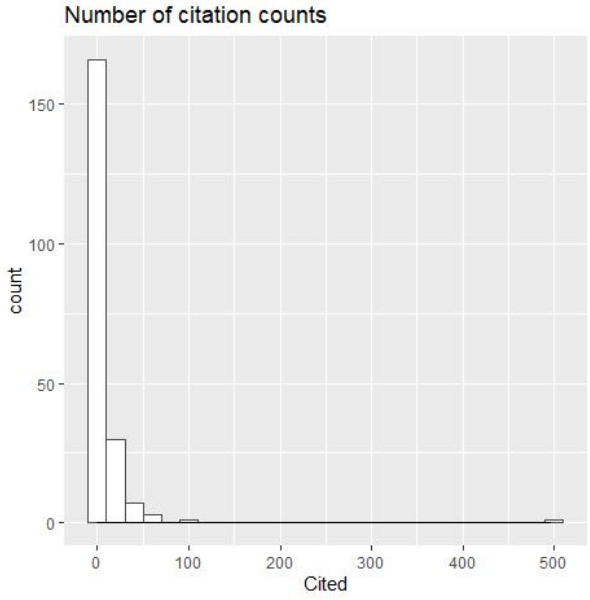

Figure 5: Number of citations of articles in the synthesis sample

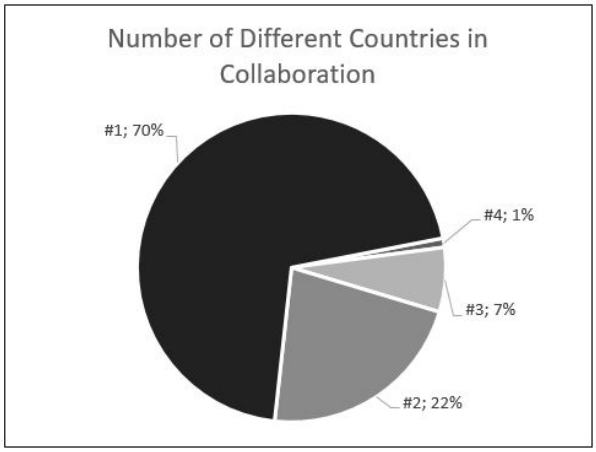

Figure 6: Number of distinct collaborating countries for papers in the synthesis sample

Table 1: Network Basic parameters

Measure	**Value**
Number of Nodes	45
Number of Edges	116
Average Degree	5,156
Avg. Weighted Degree	136,356
Network Diameter [19]	4
Graph Density	0,117
Modularity [20]	0,442
Number of Communities	12
Avg. Clustering Coef.	0,497
Avg. Path Length	2,341

laboration, while close to 1% of the papers in the sample result of researchers in 4 countries collaborating, the highest number of distinct collaborating countries [13]. [14].

Countries in the sample produced papers with collaboration, without collaboration, or both. As shown in Figure 7 USA is the country that has produced the most papers about cyber-resilience framework with 73, with almost two-thirds of them authored by researchers associated with institutions in the USA. As a result, USA is the country with the least proportion of research collaboration in our sample. On the other hand, Chinese researchers have produced more articles through international collaboration than through research merely between Chinese researchers. Figure 7 reflects the countries that were predominantly collaborative and non-collaborative ordered by the number of papers from that country in the synthesis sample. For this analysis, if an article has been published by scientists in two countries for example, it will appear once for each country. The total number therefore reflects the number of distinct researchers that authored the papers in the synthesis sample.

The network representation of the authors involved in the production of articles in the synthesis sample is shown in Figure 8, through use of an undirected graph. The main parameters that describe this network are listed in Table 1.

A clustering analysis of this network of authors shows one big cluster around the US and China, smaller peripheral clusters of European countries collaborating with south-east Asia, and several countries that have not collaborated internationally, and appear as isolated islets in a network representation. Notable examples of these lack of collaboration include Japan with four CRF papers [15], [16], [17] and [18].

Figure 9 shows a measure of the efficiency in the article production process per country,

Non-Collaborative

Country	Coll.	Non-Coll.	Total
USA	25	48	73
England	6	9	15
India	6	7	13
France	4	4	8
Japan	0	4	4
Ireland	1	2	3
Greece	1	2	3
Iran	1	2	3
Jordan	0	2	2
Thailand	1	1	2
Malaysia	0	2	2
North Ireland	0	1	1
Macedonia	0	1	1
Turkey	0	1	1
Romania	0	1	1
South Africa	0	1	1
Wales	0	1	1
Mexico	0	1	1
Total	**45**	**90**	**135**

Collaborative

Country	Coll.	Non-Coll.	Grand Total
Peoples R China	22	21	43
Australia	7	6	13
Singapore	7	3	10
Canada	5	4	9
Germany	7	2	9
South Korea	4	3	7
Italy	5	2	7
Sweden	4	2	6
Saudi Arabia	3	2	5
Israel	5	0	5
Portugal	2	1	3
Denmark	3	0	3
Switzerland	2	1	3
Brazil	2	1	3
Taiwan	2	0	2
Luxembourg	2	0	2
Pakistan	2	0	2
Spain	2	0	2
Poland	1	0	1
Kazakhstan	1	0	1
Qatar	1	0	1
Netherlands	1	0	1
Norway	1	0	1
Ukraine	1	0	1
Austria	1	0	1
Hungary	1	0	1
U Arab Emirates	1	0	1
Ghana	1	0	1
Myanmar	1	0	1
Total	**97**	**48**	**145**

Figure 7: Number of author by country of association and collaboration status

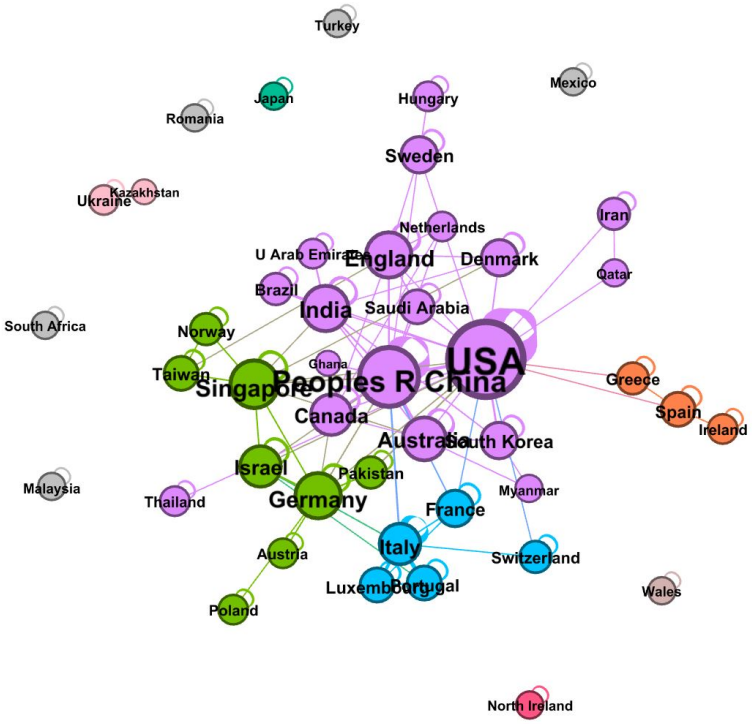

Figure 8: Network representation of author collaborations

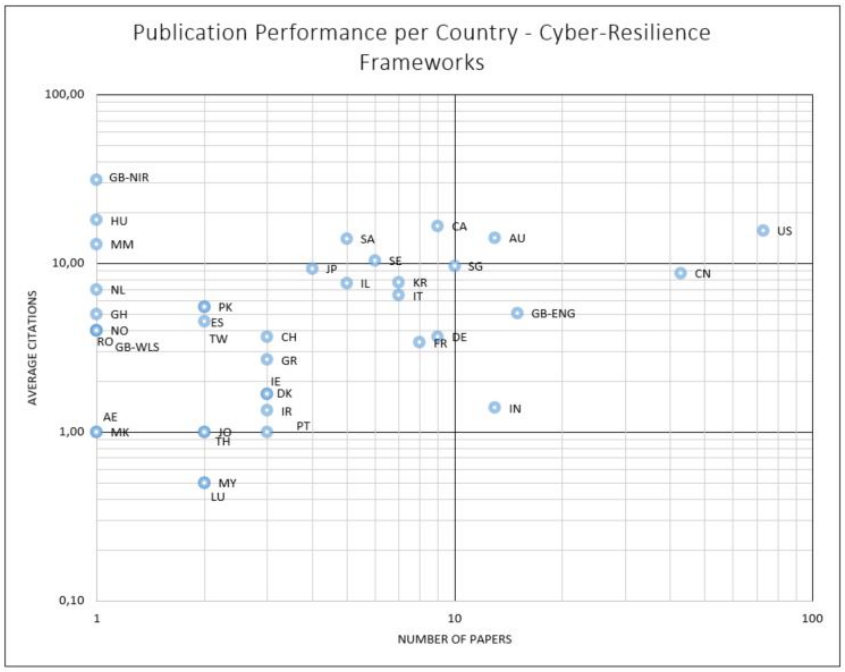

Figure 9: Articles versus citations per country in the sample

represented through the relationship between articles produced and citations per article. The US is positioned as the country with both a high production of CRF articles and a high number of average citations, followed closely by China, with Australia and England following further behind.

4 Text and clustering analysis

Our team carried out a text and clustering analysis of the papers in the `synthesis sample` by analysing the words in their titles and abstracts. Abstracts have an average length of 179 words with a minimum of 26 and a maximum of 443 words. Figure 10 shows the distribution of abstract lengths in the sample. This variability is partly attributable to the wide range of journals where these articles have been published, as presented in Figure 4.

A detailed analysis of the word frequency in the abstracts is represented in the word cloud shown in Figure 12. This word cloud is obtained through the use of R's `wordcloud` package, after the data has been stemmed and lemmatized by using the `textstem` package.

A clustering of the same data results in the figure shown in Figure 11. The divisive hierarchical clustering method is used, which performs an iteration which starts with all articles members of one cluster, and which then divides the most heterogeneous cluster into two clusters, a process that is continued until every member of the set is in its own cluster. The R package used for this analysis, `stats`, uses the Ward minimum variance method to determine the distance between the existing clusters to determine the next cluster that is to be subdivided next [21].

This figure highlights the three main clusters in the data, and the words that are most often present in the abstracts of each of the clusters. The clusters present clear differences between them. The first cluster centers around the concepts of `system`, `cyber`, and `attack`, relating to articles with frameworks for systemic cyber attacks. A second cluster has a greater number of concepts that cluster together, where concepts like `control` and `network` stand out. A third cluster, showing the greatest number of concepts, gathers the greater incidence of words such as `simulation`, `technology`, `design` and `strategy`.

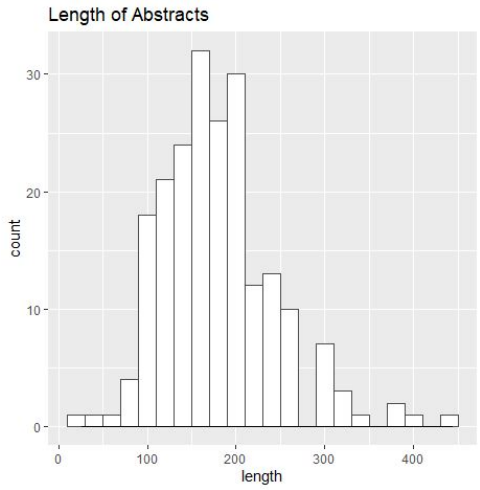

Figure 10: Abstract word length in sample

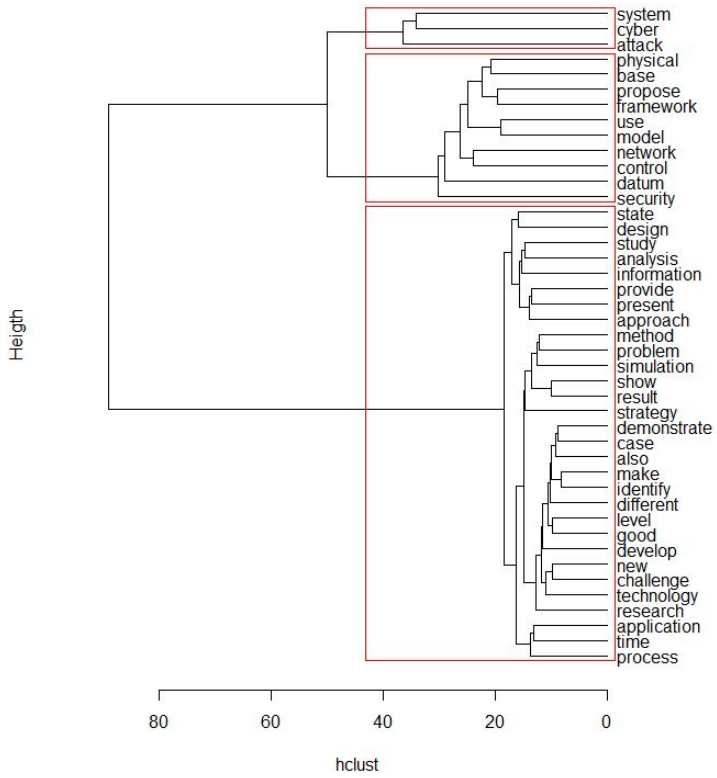

Figure 11: Clustering of abstract texts in sample, Ward method

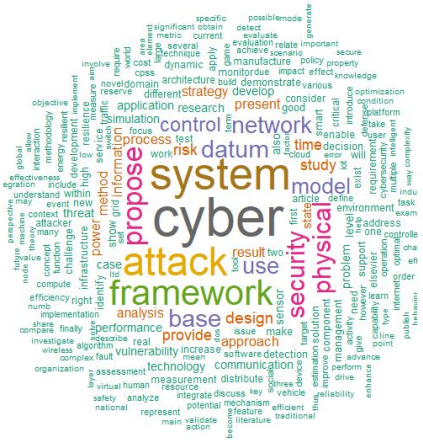

Figure 12: Word cloud from word frequencies in sample abstracts

5 Thematic analysis

The thematic analysis in this paper categorizes the articles in the `synthesis sample` according to characteristics of the frameworks these articles present and/or implement, as a way of answering the research questions of this paper. The categorizations that have been used for this analysis are:

- Resilience time frame and hierarchy category to which the frameworks belong,
- The industrial area where the cyber resilience frameworks are applied,
- The types of attacks that each of these frameworks address,
- The methods used in these frameworks, and
- The countries and organizations (e.g., institutes, universities) where this research is taking place.

A first categorization used corresponds to the resilience framework presented by Guerra & Sepulveda Estay [22], corresponding to the `"Wave Analogy"` for resilience, which categorizes resilience frameworks along an event timeline which has a disruption event at its center, with categories grouping frameworks lead to the disruption and categories grouping frameworks that follow from the disruption, from operational to strategic.

The categorization proposed by Guerra & Sepulveda-Estay considers twelve categories according to a dynamic and a hierarchical dimension. The dynamic dimension groups articles according to the time at which decisions can be made about resilience for each category, either before, during, or after the disruption. The hierarchical dimension categorizes the level at which the decisions are made about resilience, either at a strategic or at an operational level. The categories and dimensions contained in the *Wave Model* are illustrated in Figure 13.

Figure 14 shows the number of articles in the synthesis sample for each of the *Wave Analogy* categories. One paper may have had more than one category, although in those cases categories are normally hierarchically close to each other. The biggest share of the papers in the sample are in the category of Pre-event Knowledge Management, and concerning risk analysis, simulation and modeling. Examples of papers in the different Wave Analogy categories are shown in Table 2. The category with most papers is the *Pre-event Knowledge Management* followed by *Security*, *Velocity*, and *Ability to Adapt*.

The research areas represented in the `synthesis sample` papers are listed in Table 3, with examples of papers for the main research areas and application areas found in the synthesis sample.

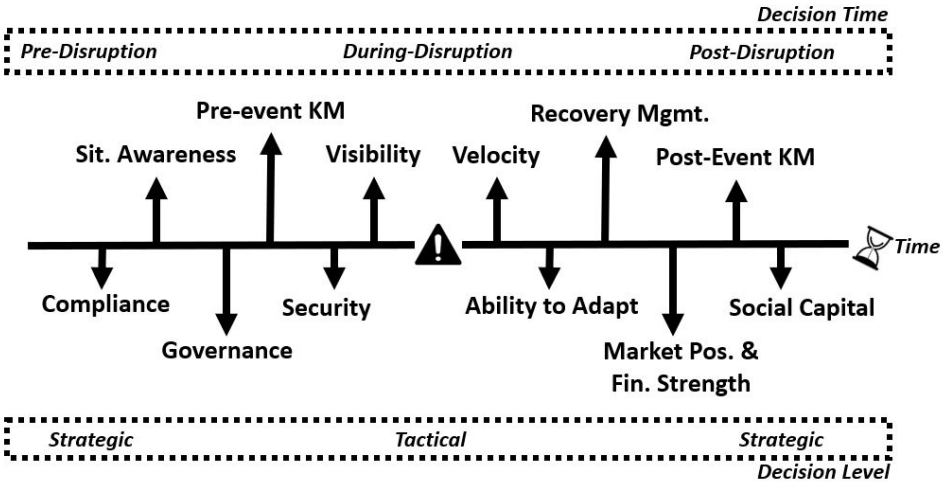

Figure 13: Categorization of resilience frameworks according to the *Wave Analogy* [22]

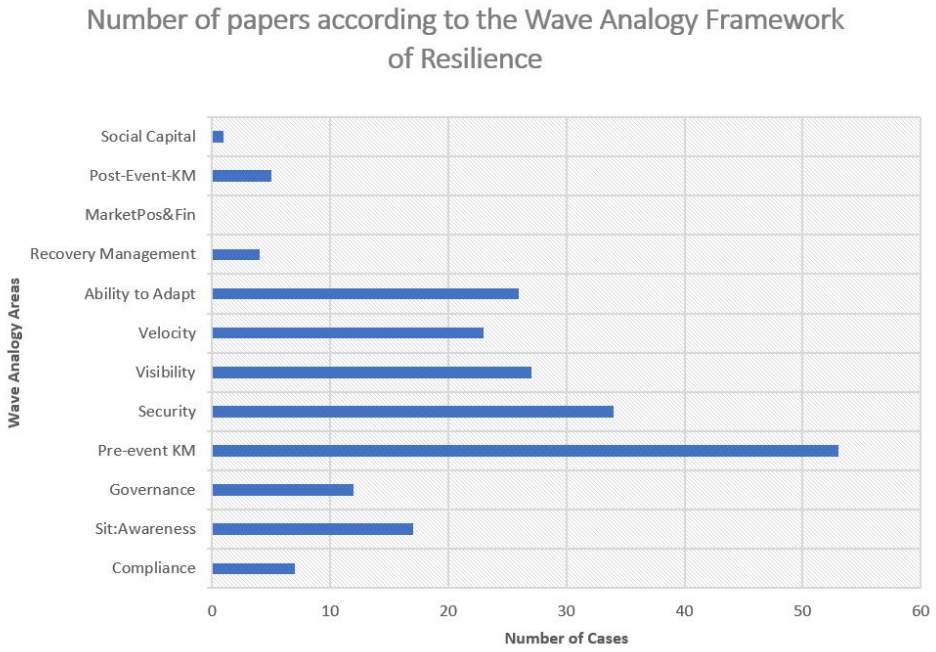

Figure 14: Papers in the synthesis sample according to the *Wave Analogy* for resilience

Table 2: CRF examples from synthesis sample for every Wave Analogy Category

Wave Analogy Category	Example papers
Compliance	[23] [24] [25]
Situational Awareness	[26] [27] [28] [29] [30]
Governance	[31] [32] [33] [34] [35] [36] [37]
Pre-event Knowledge Management	[26] [38] [39] [40] [41] [42] [43][44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54]
Security	[55] [56] [57] [58] [59] [11] [60] [61] [62]
Visibility	[17] [63] [12] [64] [65]
Velocity	[66] [67] [68] [69] [70]
Ability to Adapt	[71] [70] [72] [73] [74] [75]
Recovery Management	[76] [77] [1] [78]
Market Position and Finance	*No papers found in sample*
Post-event Knowledge Management	[79] [80] [81] [15] [10]
Social Capital	[28]

A network analysis of these areas with respect to the countries where these areas have been researched is shown in Figure 15.

Several of the papers in the `synthesis sample` indicated a specific cyber-attack. The types of attacks that have been addressed in the papers in the `synthesis sample` are presented in Table 4.

The attack type that is mentioned the most in the papers in the sample are are the False Data Injection Attacks (FDIA), followed by the Distributed Denial of Service (DDOS).

The cyber-resilience frameworks presented in the papers in the `synthesis sample` use a number of different methods in the CFR's that are proposed. Table 5 lists the methods that have been found in the `synthesis sample` and the institutions that are using these methods, referencing example papers. The categorization structure is based on the main method used for each paper in the sample. The number of methods used have been categorized as either related to Algorithms, Game theory, Architecture, Optimization, Machine learning, Statistical methods, Qualitative methods and Simulation. Machine learning and Optimization were shown separately to be able to include sub-classes of these categories. The same reasoning is applied for separating game theory from algorithms, for example.

The research institutions with the highest number of CRF-related paper publications in the sample are headed by the University of Illinois in the US with 6 publications, followed by Northeastern University located in China and the University of Wisconsin in the US with 5 publications each. The methods that present the highest number of references is *General risk Assessment*, followed by *Bayesian Networks* and *Machine Learning*.

Table 5: CRF examples from synthesis sample for methods used and organizations using them

General Method	Specific Method	Research Institution
Algorithms	Attack graphs and attack trees	Univ Warwick,UK[130]
	Attack resilient	PNNL,US & Iowa state Univ,US & Argoinne Nar Lab,US[62]

Continued on next page

Table 5 – continued from previous page

General Method	Specific Method	Research Institution
	Candidate in-variants	Univ texas,US & Vanderbilt Univ,US[98]
	Contradiction Methods	Yangzhou Univ,CN & Brunel Univ,UK & King Adbulaziz Univ,SA[131]
	Control based mitigation	Univ Toronto,CA & TELUS Comun,CA[104]
	Cooperative Observer-based detection	NUS,SG & IIT Dehli,IN & Aalborg,DK[97]
	Doubly weighted trees	George Mason Univ,US & US NAval Acad,US & Chiang Mai Univ,TH[60]
	Dynamic State Estimator	Univ Texas,US & Argonne Nat Lab,US & Purdue Univ,US[110]
	Dynamic Watermarking	Texas A&M Univ,US[44]
	Efficient Data Recovery	Japan Adv Inst Sci&Tech,JP[15]
	Graph Theoretic characterization	Univ California St Barbara,US[12]
	Inference system synthesis	Univ Hong-Kong,CN & Michigan Tech Univ,US & Waterfall Secur Solut,IL[106]
	Kullback Leibler divergence	Northeastern Univ,CN[129]
	Matrix decomposition & Factorization	Shanghai Jiao Tong Univ,CN & Chinese Acad Sci,CN & Xian Jiaotong Liverpool Univ,CN & Univ Coll Eng,IN[48]; Rensselaer Polytech Inst,US & Exponent Inc.,US & New York Power Author,US[103]
	Real time traffic analysis	Cardiff Univ,UK[50]
	Software Defined Networking (SDN)	Embry Riddle Aeron Univ,US[71]; Tech Univ Danmark,DK[125]
Architecture	Adaptive base corrective signal	Amirkabir Univ Tech,IR & Qatar Univ,QA & Georgia Inst Tech,US[27]
	Artificial Immune server	Kanagawa Inst Tech,JP[18]
	Co-design	Daegu Gyeongbuk Inst Sci Tech,KR[55]
	Discrete event triggered communication	Lanzhou Univ Tech,US[83]
	Dist. Kalman Fusion Estimator	City Univ Hong-Kong,CN & Nanyang Tech Univ,SG & Zhejiang Univ Tech,CN[61]
	Systems Design	Carnagie Mellon Univ,US & Univ Virginia,US[11]
	Three-layered reference architecture	Washington State Univ,US & MITRE Corp,US & Univ Texas,US[105]
	Variable structure system theory	Commun Univ China,CN & Texas A&M Univ,US & Univ Toronto,CA[112]
Game Theory	Bi-linear differential quality	Caspian State Univ,KZ & European Univ,UA [80]
	Nash Equilibrium	Univ Sydney,AU & Univ New South Wales,AU[113]; Hong-Kong Univ,CN & Zhejiang Univ,CN & Univ. Newcastle,UK [94]; Univ Bristol, UK[64]
	Two-stage Min-Max	ETH,CH & Univ Tech Sydney,AU[75]

Continued on next page

Table 5 – continued from previous page

General Method	Specific Method	Research Institution
Literature Review	General	Tech Univ Denmark,DK[1]; Univ Murcia,ES & Univ Aegean,GR[132]; Univ of Tech,MY[53]
	Regulation	Jundal Global Univ,IN & Int Inst Informat Technol,IN[23]; Macquarie Univ,AU[31]
	Security Objectives	Beijing Univ,CN[133]
	Taxonomy & Propagation	Univ Oxford,UK[51]
Machine Learning	General	NUST,PK & Fontbonne Univ,US & IIUI,PK[38]; Zhengzhou Int Informat Sci & Tech,CN[56]; UTP Univ Sci Technol,PL & Fern Univ,DE[134]; Thapar Univ,IN[79]; Northeastern Univ, CN[128]
	Data Mining and Classification	Univ Tun Hussein Onn,MY[68]
	Deep Learning	Illinois State Univ, US & Univ Texas, US[135]
	Robust Regression	Takyo Inst Tech,JP[17]
	Text Analysis - Nat. Lang. Proc.	Christ Univ,IN[30]
Maturity Model	Cloud Based	Univ Tech Sydney,AU[37]
Optimization	Bi-level MILP	Hunan Univ,CN & Illinois Inst Tech,US[99]; New York Univ,USA[34]
	Markov chains - Dyn Prog	Beijing Inst Tech,CN[117]; Univ Wisconsin,US & Univ Toledo,US & ATSEC Informat Secur Corp,US[114]
	Min-Max Multi-obj	Queen Mary Univ London,UK[136]
	Parametric fb linearization	Univ Toronto,CA[104]
	Semi-Definite Programming	Univ Calif Berkeley,US & KTH Royal Inst Tech,SE [108]
	Stochastic model	IBM Corp,US & Southern Method Univ, US[33]
Qualitative	Rational Choice perspective	Temple Univ,US[63]
	Vulnerability detection	Rangsit Univ,TH[52]
Risk Assess.	General	Univ Roma,IT[96]; Univ Plymouth,UK[40]; Deakin Univ,AU & Univ Kentucky,US[41]; Chinese Acad Sci,CN[42]; Univ Roma,IT & Univ Coimbra,IT & Israel Elect Corp Ltd, IL[115]; UNIST,KR[43]; Air Force Inst Tech,US & Appl Res Solut,US & LGS Innovat,US[121]; DoD Nat Def Univ,US[88]
	Economic Evaluation	Univ Virginia,US[9]
	Satisfiability Module theory	Univ North Carolina,US[59]
	Tallin Manual	Korea Univ,KR[102]
	Vulnerability Management	Univ Luxembourg,LU & Itrust Consulting,LU & Roma Tre Univ,IT & CRAT,IT & Univ Coimbra,IT & Leonardo SpA,IT[58]

Continued on next page

Table 5 – continued from previous page

General Method	Specific Method	Research Institution
	Interdependency	Univ Newcastle,AU & Chinese Univ Hong-Kong,CN & China Southern Power Grid,CN & Univ Sydney,AU & Chongquing Univ,CN & Univ New South Wales,AU[109]
Simulation	Agent-based system	Hacettepe Univ,TR[66]
	Ad hoc on demand distance vector	Jaypee Univ Inf Tech,IN & Vellore Inst Tech,IN & Soonchunhyang Univ,KR & La Trobe Univ,AU[116]
	Bayesian Max. Likelihood Est.	Univ Georgia,US[45]
	Bayesian Networks	Univ Limerick,IE[123]; George Mason Univ,US[76]; Benedict Coll,US & Univ Illinois,US[69]; Missouri Univ Sci Tech,US[81]; World Islamic Sci Edic Univ,JO & Royal Jordanian Air Forces,JO[89]
	Block-chain	Chinese Univ Hong-Kong,CN & Univ Sci Tech China,CN & Univ Newcastle,AU & Univ Sydney,AU & Chongqing Univ,CN & Elect Power Res Inst,US & Univ South Wales,AU[109]
	BMI Control	Univ Luxembourg,LU & Univ Lorraine,FR[118]
	Bounded sensor reading	Nanyang Tech Univ,SG[47]
	Convex Optimization	South China Univ Tech,CN[127]
	Distributed Attack	Iran Sci Univ Tech,IR[54]
	Hierarchical Modeling	MIT,US[77]
	LiSM: Land in Sand Miner	NEC Labs Amer,US & Univ Illinois,US & BBN Tech,US[86]
	Montecarlo	Politech Milan,IT & Univ Paris,FR[48]
	Penetration Testing	Malek Ashtar Univ Tech,IR & NIOPDC,IR[26]; US Air Force,US[29]
	Process	Northeastern Univ,CN[128]; Singapore Univ Tech Design,SG & Optiwater,IL & Technion Israel Inst Tech,IL[49]; Shenandoah Res Tech,US[90]
	Reliability	Univ Idaho,US & Texas A&M Univ,US[57]
	Robust predictive control	Northeastern Univ,CN[119]
	Stochastic methods	Arizona State Univ,US & Penn State Univ,US & Swiss Fed inst Tech,CH[74]; Jiangnan Univ,CN & Northeastern Univ,CN[126]
	Swarming Based Cyber Defense	Mil Acad Gen Mihailo Apostolski,MK[91]
	Traffic Flow - Lighthill-Whitham-Richards	King Abdullah Univ Sci Tech,SA & Univ Califonia Berkeley,US[65]
Statistical	Honeypot	Univ Texas,US & Illinois State Univ,US[137]; Ben gurion Univ,IL & Deutsch Telekom,DE & Bosch Ctr Artif Intel,DE[28]
	Hypothesis Testing	Univ Florida,US & Univ Sao Paulo,BR[70]

Continued on next page

Table 5 – continued from previous page

General Method	Specific Method	Research Institution
	Modeling	Charles Darwin Univ,AU & Univ Melbourne,AU & Commonwealth Bank,AU[95]
Strategy	Attack Strategy	Singapore Univ Tech Design,SG & Univ Oslo,NO & Nat Tsing Hua Univ,TW & Nat Chiao Tung Univ,TW & Nat Sun Yat Sen Univ,TW[107]
	Criminal Law	Yale Univ,US & Princeton Univ,US[36]
	Critical infrastructure Regulation	Univ Petr&En Studies,IN & Wipro tech,IN[35]
	Cyber-crime	Univ Portsmouth,UK & Lund Univ,SE & Athabasca Univ,CA[10]
	Hierarchical Contracts	Nanyang Tech Univ,SG & Delta Elect,SG[73]
	Regulation Instrument Comparison	Univ Leeds,UK[24]
	Two-pronged	CUST,PK & Univ Bremen,DE & BIBA Bremer Int Prod,DE & Bahria Univ,PK[84]
Survey	General	Shanghai Univ,CN[67]; Univ Hull,UK[92]; MIT,US[82]

6 Analysis and future work

The papers in the sample evidence both the increasing interest that cyber resilience frameworks is receiving in academic research, and the variety of approaches that are being proposed to understand how a CRF can be designed and implemented. The approach variety is reflected at least in the the number of different attacks that are addressed in the CRFs proposed, and in the methodologies that are used.

Out of the 136 journals included in the paper sample, 20% of the journals only contain 92 articles (44,2% of the total). This high dispersion in the publication density is an indication that there is as yet no clear focus for the research of CRF. This can also be understood from the number of different areas (25) where this research is taking place.

The categories proposed by the *wave Analogy* model as presented in Figure 13 facilitate a relevant structure for the description, from the papers in the `synthesis sample`, of the current state of CRF research. According to Figure 14 the category with most `synthesis sample` publications is *Pre-event knowledge Management*, which considers the risk analysis of vulnerabilities and their economic, legal and operational implications. The categories that follow it in number of `synthesis sample` papers addressing the *Security* of Cyber-Physical systems, the *Visibility* of cyber-Physical systems and their *Adaptability* once the events have occurred.

This category analysis also shows that most of the research has been focused in operational aspects of cyber resilience, with only a few articles in the `synthesis sample` about the more strategic *Governance* or *Social Capital*. The relative difference in numbers between CRF papers about Strategy with respect to Operations is a reflection of the preferred approach for containment of disruptions from cyber-attacks by using a CRF, this is mainly in the operational plane rather than an approach of design for avoidance or for the response to disruptions.

Multiple operational disruptions originating from cyber-attacks are strong evidence that response and recovery from a cyber-disruption is not the last resource when prevention has

Table 3: CRF examples from synthesis sample for research and application areas

Research Areas	**Application Areas**
Computer Science	Cloud Technology [37] [81]
	Cyber attack outsourcing [82]
	Manufacturing [83] [71] [84]
	Military Operations [76] [52] [85] [86] [87] [75] [88] [89] [77] [29] [90] [91] [92]
	Networks [64] [54] [50] [93] [94] [33] [42]
	Social Networks [28]
	Software Development [95]
	Web-based platforms [96] [18]
Engineering	Electrical Grids [97] [98] [99]
	Food Production [100]
	Pharmaceutical [66]
	Nuclear Plants [101] [43] [102]
	Oil and Gas [26]
	Power Systems (Electrical) [103] [104] [17] [105] [106] [68] [107] [108] [109] [72] [110] [111] [57] [62] [112]
	Smart Grid [70] [48] [113] [45] [114]
	Water Distribution [49]
Telecommunications	Communication Network [32] [15] [65] [115]
	Cyber Forensics [79]
	Healthcare [116]
	Wireless Networks [46] [117] [55] [16]
Automation & Control Systems	Adaptive Control [27]
	Distributed Control [67]
	General Control [118] [81] [13] [119] [39] [58]
Government & Law	Critical Infrastructure [41] [11] [91]
	Finance [38] [31]
	Foreign Policy [120]
	Legal [36]
	Regulation [35] [23] [24]
Business and Economics	Economics [25]
	Insurance [34] [121]
	Intellectual Property [9]
	Supply Chains [1] [78]
Public Administration	Public Sector [122]
	National Power Systems [63]
	Critical Infrastructure [11]
Transport	Autonomous Vehicles [123] [124]
	Shipping [40] [125]
	Transportation Networks [69] [80]

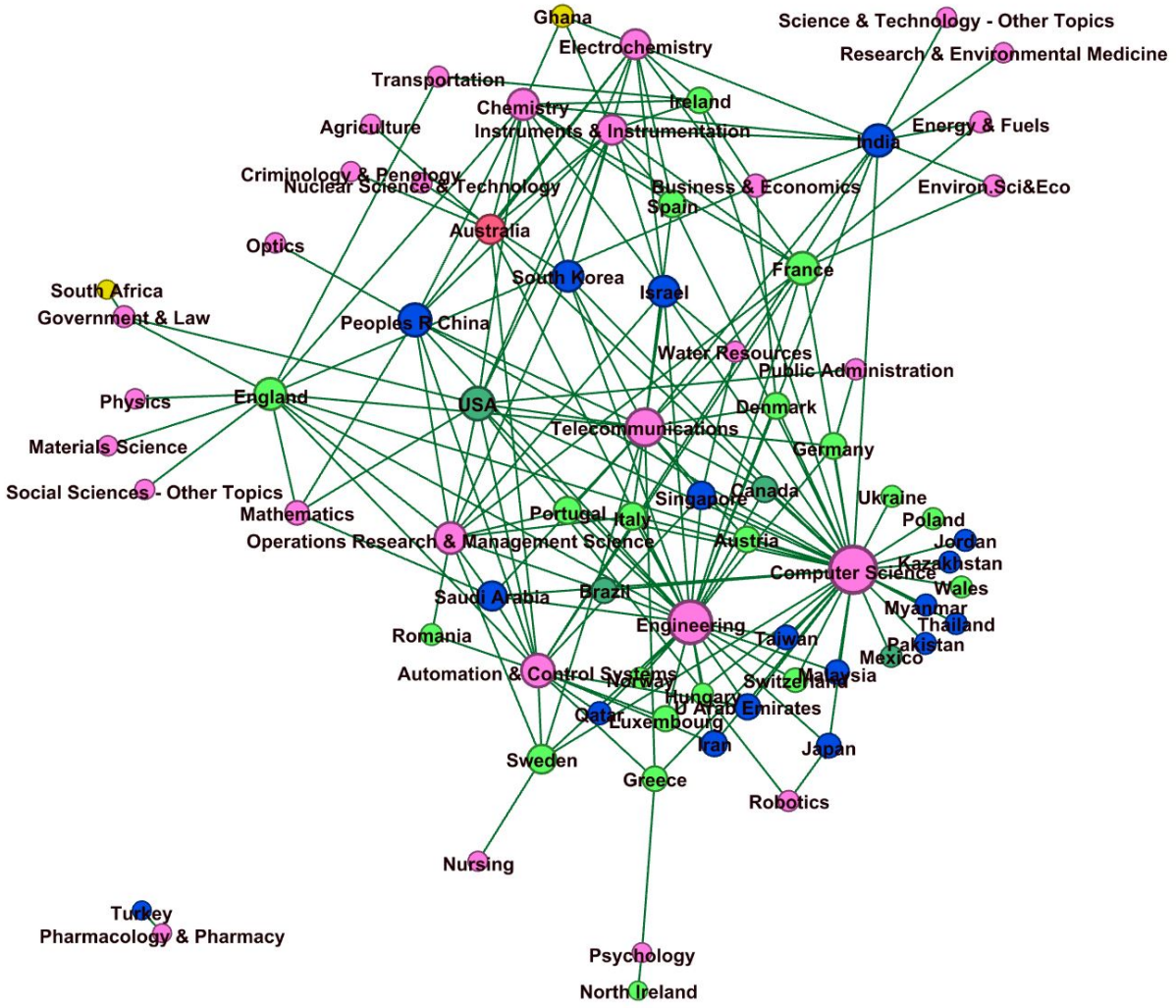

Figure 15: Network analysis of Countries and Research Areas in sample

Table 4: CRF examples from synthesis sample for cyber attack types and application areas

Attack Type	**Application areas**
Actuator Attacks	Manufacturing [83]
	Adaptive Control [27]
Advanced Persistence Attacks	Social Networks [43]
Alter and Hide	Power Systems (electrical) [106]
Authentication & Availability	Manufacturing [84]
Black Hole & Grey Hole	Healthcare [116]
Deception	Non-specific CPS [126] [39]
	Power Systems (electrical) [107]
	Smart Grid [70]
	Switching [112]
Distributed Denial of Service (DDOS)	General Control [119] [127]
	Government Regulation [23]
	Networks [93] [94] [64] [125]
	Non-specific [128]
	Wireless Networks [117]
False Data Injection (FDIA)	Electrical Grids [97] [99] [98]
	Non-Specific CPS [129] [74]
	Power Systems (electrical) [108] [109] [72] [99] [110] [111]
	Smart Grid [45] [114]
Ransomware	Finance [31]
Replay	Non-specific CPS [61]
Sensor-related	Alterations [126] [47]
Spoofing	Communication Networks [65]
Stealth	Electrical Grids [97]
Zero-Day	Power Systems (electrical) [68]
	Software Development [95]

failed, but in many cases is a strategy in itself, particularly when dealing with systems that are so complex that it is infeasible to analyze and prevent every way in which the system can fail.

The collaboration between countries in the development of CRFs was also found to be a relevant difference between the papers in the `synthesis sample`. A majority of the researcher countries in the sample, 61,7%, have chosen to collaborate in the development of CFRs, as can be seen in Figure 7. Only 17% of the researcher countries carried out exclusively non-collaborative papers, while in contrast 31% of the researcher countries delivered exclusively collaborative research. It is the understanding of this team that a de-centralized problem such as cyber-attacks with operational disruption not only needs a global approach to respond to the effects of these attacks, but also will benefit from multiple points of view in order to propose effective and innovative CRFs. Some of the

In regard to the opportunities for collaboration, this paper provides both an introductory overview of the CRFs as proposed in literature and a categorization of these CRFs, as enablers for collaboration. The industry areas are presented in Table 3 , Table 4 presents the attacks that are addressed in current CRFs, and Table 5 lists the methods used and the research institutions using these methods.

The analysis shown in this paper makes evident that a future deeper look is possible, for an analysis of CRFs in specific methodological areas, industrial applications or related to specific attack types, for example.

The network analysis that has been explored in this paper is a way of representing the relationships between countries and their collaborations in Figure 8 or countries and their research areas in Figure 15 represent quantitatively the current state of the relationships found in the `synthesis sample`. As shown in Table 1, a network analysis found 12 relevant communities, with an *Average Clustering Coefficient* o 0,497, meaning that on average nodes are connected to 49% of all the nodes in the network. This average connectivity is driven by highly connected nodes (countries) like USA and China, which compensate for isolated nodes such as South Africa or North Ireland, for example. This contrast between highly connected nodes and nodes with a low connection can be seen in the *Graph Density* measure with a value of 0,117, meaning that only 11,7% of all possible connections are present in the network.

The work presented in this paper has followed a rigorous, structured approach to the gathering and analysis of information to advance the knowledge about CFR's. However, in future other sources of knowledge should be used, particularly when considering a rapidly developing area such as cyber-resilience. In the process of gathering the sample that has been analyzed and presented in this paper, our team found numerous reports by private institutions about the proposal of CRFs. These data sources have not been included in this review, as they are not peer reviewed. However, these are important references to the industrial application of CRFs. It is not clear how these reports eventually become scientific, published, peer-reviewed work. Due to the rapid development of the topic of cyber resilience, future scientific work should both address the proposal of methods to use information contained in industrial reports, to counter act the existing relatively slow publishing cycles.

References

7 References

[1] O. Khan and D. A. Sepulveda Estay, "Supply chain cyber-resilience: Creating an agenda for future research," *Technology Innovation Management Review*, no. April, pp. 6–12, 2015.

[2] Google Trends, "Google trends report for term "cyber resilince"," 2019. https://trends.google.com/trends/explore?date=allq=%2Fg%2F11c3ypk3jn, Last accessed on 2019-11-26.

[3] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd., 2006.

[4] G. Schryen, G. Wagner, and A. Benlian, "Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of is literature," in *Proceedings of the Thirty Sixth International Conference on Information Systems, Fort Worth*, 2015.

[5] C. F. Durach, J. Kembro, and A. Wieland, "A new paradigm for systematic literature reviews in supply chain management," *Journal of Supply Chain Management*, vol. 53, no. 4, pp. 67–85, 2017.

[6] C. D. Mulrow, "The medical review article: state of the science," *Annals of internal medicine*, vol. 106, no. 3, pp. 485–488, 1987.

[7] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," *British journal of management*, vol. 14, no. 3, pp. 207–222, 2003.

[8] K. Ebata, Y. Watanabe, Y. Nezu, and S. Tanimura, "Cyber attack countermeasures based on websam incidentguard and authentication switches," *NEC technical journal*, vol. 1, no. 1, pp. 28–31, 2006.

[9] E. Andrijcic and B. Horowitz, "A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property," *Risk analysis*, vol. 26, no. 4, pp. 907–923, 2006.

[10] V. Katos and P. M. Bednar, "A cyber-crime investigation framework," *Computer Standards & Interfaces*, vol. 30, no. 4, pp. 223–228, 2008.

[11] C. G. Chittister and Y. Y. Haimes, "The role of modeling in the resilience of cyberinfrastructure systems and preparedness for cyber intrusions," *Journal of Homeland Security and Emergency Management*, vol. 8, no. 1, 2011.

[12] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[13] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 1–11, 2016.

[14] C. Lv, H. Wang, B. Zhao, D. Cao, W. Huaji, J. Zhang, Y. Li, and Y. Yuan, "Cyber-physical system based optimization framework for intelligent powertrain control," *SAE International Journal of Commercial Vehicles*, 2017.

[15] N. Nower, Y. Tan, and A. O. Lim, "Traffic pattern based data recovery scheme for cyber-physical systems," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 97, no. 9, pp. 1926–1936, 2014.

[16] R. Li, J. Li, and H. Asaeda, "A hybrid trust management framework for wireless sensor and actuator networks in cyber-physical systems," *IEICE TRANSACTIONS on Information and Systems*, vol. 97, no. 10, pp. 2586–2596, 2014.

[17] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE transactions on power systems*, vol. 30, no. 5, pp. 2487–2497, 2014.

[18] M. Tarao and T. Okamoto, "Toward an artificial immune server against cyber attacks: enhancement of protection against dos attacks," *Procedia Computer Science*, vol. 96, pp. 1137–1146, 2016.

[19] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of mathematical sociology*, vol. 25, no. 2, pp. 163–177, 2001.

[20] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of statistical mechanics: theory and experiment*, vol. 2008, no. 10, p. P10008, 2008.

[21] F. Murtagh and P. Legendre, "Ward's hierarchical agglomerative clustering method: which algorithms implement ward's criterion?," *Journal of classification*, vol. 31, no. 3, pp. 274–295, 2014.

[22] P. Guerra and D. A. Sepulveda Estay, "An impact-wave analogy for managing cyber risks in supply chains," in *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, IEEE, 2019.

[23] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178–188, 2019.

[24] M. G. Porcedda, "Patching the patchwork: appraising the eu regulatory framework on cyber security breaches," *Computer Law and Security Review*, vol. 34, no. 5, pp. 1077–1098, 2018.

[25] K. Ruan, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Computers & Security*, vol. 65, pp. 77–89, 2017.

[26] M. Shakibazad, "A framework to create a virtual cyber battlefield for cyber maneuvers and impact assessment," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, pp. 1–11, 2019.

[27] M. Yadegar, N. Meskin, and W. M. Haddad, "An output-feedback adaptive control architecture for mitigating actuator attacks in cyber-physical systems," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 6, pp. 943–955, 2019.

[28] A. Paradise, A. Shabtai, R. Puzis, A. Elyashar, Y. Elovici, M. Roshandel, and C. Peylo, "Creation and management of social network honeypots for detecting targeted cyber attacks," *IEEE Transactions on Computational Social Systems*, vol. 4, no. 3, pp. 65–79, 2017.

[29] E. L. Raulerson, K. M. Hopkinson, and K. R. Laviers, "A framework to facilitate cyber defense situational awareness modeled in an emulated virtual machine testbed," *Journal of Defense Modeling and Simulation*, vol. 12, no. 3, pp. 229–239, 2015.

[30] C. Cardoza and R. Wagh, "Text analysis framework for understanding cyber-crimes," *International Journal of Advanced and Applied Sciences*, vol. 4, no. 10, pp. 58–63, 2017.

[31] A. S. Irwin and C. Dawson, "Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help," *Journal of Money Laundering Control*, vol. 22, no. 1, pp. 110–131, 2019.

[32] F. Januário, A. Cardoso, and P. Gil, "A distributed multi-agent framework for resilience enhancement in cyber-physical systems," *IEEE Access*, vol. 7, pp. 31342–31357, 2019.

[33] S. Abraham and S. Nair, "Comparative analysis and patch optimization using the cyber security analytics framework," *Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 161–180, 2018.

[34] R. Zhang, Q. Zhu, and Y. Hayel, "A bi-level game approach to attack-aware cyber insurance of computer networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 779–794, 2017.

[35] V. A. Kumar, K. K. Pandey, and D. K. Punia, "Cyber security threats in the power sector: Need for a domain specific regulatory framework in india," *Energy Policy*, vol. 65, pp. 126–133, 2014.

[36] O. A. Hathaway, R. Crootof, P. Levitz, and H. Nix, "The law of cyber-attack," *Calif. L. Rev.*, vol. 100, p. 817, 2012.

[37] N. T. Le and D. B. Hoang, "Capability maturity model and metrics framework for cyber cloud security," *Scalable Computing*, 2017.

[38] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based fintech cyber threat attribution framework using high-level indicators of compromise," *Future Generation Computer Systems*, vol. 96, pp. 227–242, 2019.

[39] N. R. Rodofile, K. Radke, and E. Foo, "Extending the cyber-attack landscape for SCADA-based critical infrastructure," *School of Electrical Engineering and Computer Science; Science and Engineering Faculty*, 2019.

[40] K. Tam and K. Jones, "Macra: A model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, vol. 18, no. 1, pp. 129–163, 2019.

[41] Z. Baig and S. Zeadally, "Cyber-security risk assessment framework for critical infrastructures," *Intelligent automation and soft computing*, vol. 25, no. 1, pp. 121–129, 2019.

[42] X. Rongrong, Y. Xiaochun, and H. Zhiyu, "Framework for risk assessment in cyber situational awareness," *Iet Information Security*, vol. 13, no. 2, pp. 149–156, 2019.

[43] J. W. Park and S. J. Lee, "Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants," *Nuclear Engineering and Technology*, vol. 51, no. 1, pp. 138–145, 2019.

[44] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *Ieee Transactions on Power Systems*, vol. 33, no. 6, pp. 8345676, 6816–6827, 2018.

[45] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *Ieee Transactions on Smart Grid*, vol. 9, no. 5, pp. 7867093, 4930–4941, 2018.

[46] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 8, pp. 1049–1053, 2017.

[47] R. Su, "Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35–44, 2018.

[48] C. Wang, Y. Zhu, W. Shi, V. Chang, P. Vijayakumar, B. Liu, Y. Mao, J. Wang, and Y. Fan, "A dependable time series analytic framework for cyber-physical systems of IoT-based smart grid," *ACM Transactions on Cyber-physical Systems*, vol. 3, no. 1, pp. 7 (18 pp.), 7 (18 pp.), 2018.

[49] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *Journal of Water Resources Planning and Management*, vol. 143, no. 5, p. 04017009, 2017.

[50] M. S. K. Awan, P. Burnap, and O. Rana, "Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk," *computers & security*, vol. 57, pp. 31–46, 2016.

[51] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, 2018.

[52] A. Hemanidhi and S. Chimmanee, "Military-based cyber risk assessment framework for supporting cyber warfare in thailand," *Journal of ICT*, vol. 16, no. 2, pp. 192–222, 2017.

[53] Z. Yunos, R. Ahmad, and N. A. Mohd Sabri, "A qualitative analysis for evaluating a cyber terrorism framework in malaysia," *Information Security Journal*, vol. 24, no. 1-3, pp. 15–23, 2015.

[54] M. Ashtiani and M. Abdollahi Azgomi, "A distributed simulation framework for modeling cyber attacks and the evaluation of security measures," *Simulation*, vol. 90, no. 9, pp. 1071–1102, 2014.

[55] D. Kim, Y. Won, Y. Eun, and K.-J. Park, "Resilient architecture for network and control co-design under wireless channel uncertainty in cyber-physical systems," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 4, p. e3499, 2019.

[56] A. Ju, Y. Guo, Z. Ye, T. Li, and J. Ma, "Hetemsd: A big data analytics framework for targeted cyber-attacks detection using heterogeneous multisource data," *Security and Communication Networks*, 2019.

[57] H. Lei, Y. Chakhchoukh, and C. Singh, "Framework of a benchmark testbed for power system cyber-physical reliability studies," *International Transactions on Electrical Energy Systems*, vol. 29, no. 1, p. e2692, 2019.

[58] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. Di Giorgio, C. Foglietta, A. Galli, A. Giuseppi, F. Liberati, A. Neri, S. Panzieri, F. Pascucci, J. Proenca, P. Pucci, L. Rosa, and R. Soua, "Integrated protection of industrial control systems from cyber-attacks: the atena approach," *International Journal of Critical Infrastructure Protection*, vol. 21, pp. 72–82, 2018.

[59] M. N. Alsaleh, E. Al-Shaer, and G. Husari, "Roi-driven cyber risk mitigation using host compliance and network configuration," *Journal of Network and Systems Management*, vol. 25, no. 4, pp. 759–783, 2017.

[60] G. Agnarsson, R. Greenlaw, and S. Kantabutra, "On cyber attacks and the maximum-weight rooted-subtree problem," *Acta Cybernetica*, vol. 22, no. 3, pp. 591–612, 2016.

[61] B. Chen, D. W. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *Ieee Transactions on Cybernetics*, vol. 48, no. 6, pp. 1862–1876, 2018.

[62] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the Ieee*, vol. 105, no. 7, pp. 7936473, 1389–1407, 2017.

[63] A. Rege, "A criminological perspective on power grid cyber attacks: Using routine activities theory to rational choice perspective to explore adversarial decision-making," *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, pp. 463–487, 2014.

[64] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, "A game theoretic defence framework against dos/ddos cyber attacks," *Computers & Security*, vol. 38, pp. 39–50, 2013.

[65] E. S. Canepa and C. G. Claudel, "Spoofing cyber attack detection in probe-based traffic monitoring systems using mixed integer linear programming," in *2013 International Conference on Computing, Networking and Communications (ICNC)*, pp. 327–333, IEEE, 2013.

[66] R. V. Barenji, Y. Akdag, B. Yet, and L. Oner, "Cyber-physical-based pat (cpbpat) framework for pharma 4.0," *International journal of pharmaceutics*, 2019.

[67] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.

[68] Q. A. Al-Gburi and M. A. Mohd Ariff, "Dynamic security assessment for power system under cyber-attack," *Journal of Electrical Engineering and Technology*, vol. 14, no. 2, pp. 549–559, 2019.

[69] G. Comert, J. Pollard, D. M. Nicol, K. Palani, and B. Vignesh, "Modeling cyber attacks at intelligent traffic signals," *Transportation research record*, vol. 2672, no. 1, pp. 76–89, 2018.

[70] A. S. Bretas, N. G. Bretas, and B. E. Carvalho, "Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model," *International Journal of Electrical Power and Energy Systems*, vol. 104, pp. 43–51, 2019.

[71] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," *Computers in Industry*, vol. 104, pp. 47–58, 2019.

[72] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *Ieee Transactions on Cybernetics*, vol. 48, no. 12, pp. 3302–3312, 2018.

[73] M. S. Haque, D. Jun Xian Ng, A. Easwaran, and K. Thangamariappan, "Contract-based hierarchical resilience management for cyber-physical systems," *Computer*, vol. 51, no. 11, pp. 8625911, 56–65, 2018.

[74] S. Z. Yong, M. Zhu, and E. Frazzoli, "Switching and data injection attacks on stochastic cyber-physical systems: Modeling, resilient estimation, and attack mitigation," *Acm Transactions on Cyber-physical Systems*, vol. 2, no. 2, pp. 9 (2 pp.), 9 (2 pp.), 2018.

[75] H. Mo and G. Sansavini, "Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks," *Ieee Transactions on Reliability*, vol. 66, no. 4, pp. 1253–1265, 2017.

[76] A. B. Barreto and P. C. Costa, "Cyber-argus-a mission assurance framework," *Journal of Network and Computer Applications*, vol. 133, pp. 86–108, 2019.

[77] N. Wagner, C. Şahin, M. Winterrose, J. Riordan, D. Hanson, J. Peña, and W. W. Streilein, "Quantifying the mission impact of network-level cyber defensive mitigations," *Journal of Defense Modeling and Simulation*, vol. 14, no. 3, pp. 201–216, 2017.

[78] A. Davis, "Building cyber-resilience into supply chains," *Technology Innovation Management Review*, vol. 5, no. 4, 2015.

[79] G. S. Chhabra, V. Singh, and M. Singh, "Hadoop-based analytic framework for cyber forensics," *International Journal of Communication Systems*, vol. 31, no. 15, p. e3772, 2018.

[80] B. B. Akhmetov, V. A. Lakhno, and V. P. Malyukov, "Model of cyber security financing within the framework of the bilinear differential quality game scheme," *Radio Electronics, Computer Science, Control*, vol. 0, no. 3, 2018.

[81] B. K. Chejerla and S. K. Madria, "Qos guaranteeing robust scheduling in attack resilient cloud integrated cyber physical system," *Future Generation Computer Systems*, vol. 75, pp. 145–157, 2017.

[82] K. Huang, M. Siegel, and M. Stuart, "Systematically understanding the cyber attack business: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, p. 70, 2018.

[83] W. Li, Y. Shi, and Y. Li, "Research on secure control and communication for cyber-physical systems under cyber-attacks," *Transactions of the Institute of Measurement and Control*, p. 0142331219826658, 2019.

[84] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Computers in Industry*, vol. 97, pp. 132–145, 2018.

[85] D. E. Denning, "Framework and principles for active cyber defense," *Computers & Security*, vol. 40, pp. 108–113, 2014.

[86] L.-A. Tang, X. Yu, Q. Gu, J. Han, G. Jiang, A. Leung, and T. L. Porta, "A framework of mining trajectories from untrustworthy data in cyber-physical system," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 9, no. 3, p. 16, 2015.

[87] V. Jaquire and B. von Solms, "A strategic framework for a secure cyberspace in developing countries with special emphasis on the risk of cyber warfare," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 5, no. 1, pp. 1–18, 2015.

[88] J. Q. Chen, "Deception detection in cyber conflicts: A use case for the cybersecurity strategy formation framework," *International Journal of Cyber Warfare and Terrorism*, vol. 6, no. 3, pp. 31–42, 31–42, 2016.

[89] I. Atoum and A. Otoom, "Effective belief network for cyber security frameworks," *International Journal of Computers*, vol. 11, pp. 117–22, 117–122, 2017.

[90] D. L. Bergin, "Cyber-attack and defense simulation framework," *Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 383–392, 2015.

[91] M. Hadji-Janev and M. Bogdanoski, "Swarming-based cyber defence under the framework of collective security," *Security Journal*, vol. 30, no. 1, pp. 39–59, 2017.

[92] A. Alqahtani, "Towards a framework for the potential cyber-terrorist threat to critical national infrastructure," *Information and Computer Security*, vol. 23, no. 5, pp. 532–569, 2015.

[93] Y. C. Sun and G. H. Yang, "Event-triggered resilient control for cyber-physical systems under asynchronous dos attacks," *Information Sciences*, vol. 465, pp. 340–352, 2018.

[94] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 7172466, 2831–2836, 2015.

[95] M. Tang, M. Alazab, Y. Luo, and M. Donlon, "Disclosure of cyber security vulnerabilities: time series modelling," *International Journal of Electronic Security and Digital Forensics*, vol. 10, no. 3, pp. 255–275, 2018.

[96] P. Russo, A. Caponi, M. Leuti, and G. Bianchi, "A web platform for integrated vulnerability assessment and cyber risk management," *Information*, vol. 10, no. 7, p. 242, 2019.

[97] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[98] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on industrial informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[99] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model," *Ieee Transactions on Smart Grid*, vol. 9, no. 2, pp. 1534–1536, 2018.

[100] J. West, "A prediction model framework for cyber-attacks to precision agriculture technologies," *Journal of Agricultural & Food Information*, vol. 19, no. 4, pp. 307–330, 2018.

[101] W. Wang, A. Cammi, F. Di Maio, S. Lorenzi, and E. Zio, "A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants," *Reliability Engineering & System Safety*, vol. 175, pp. 24–37, 2018.

[102] K.-b. Lee and J.-i. Lim, "The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd.," *KSII Transactions on Internet & Information Systems*, vol. 10, no. 2, 2016.

[103] P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of successive "unobservable" cyber data attacks in power systems through matrix decomposition," *IEEE Transactions on Signal Processing*, vol. 64, no. 21, pp. 5557–5570, 2016.

[104] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1846–1855, 2015.

[105] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, 2011.

[106] C. Wang, C. W. Ten, Y. Hou, and A. Ginter, "Cyber inference system for substation anomalies against alter-and-hide attacks," *Ieee Transactions on Power Systems*, vol. 32, no. 2, pp. 7484326, 896–909, 2017.

[107] H. M. Chung, W. T. Li, C. Yuen, W. H. Chung, Y. Zhang, and C. K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 8435933, 4577–4588, 2019.

[108] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid ac-based state estimation: Vulnerability analysis against cyber attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 8403288, 1784–1799, 2019.

[109] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 8118126, 1704–1712, 2019.

[110] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886–899, 2018.

[111] J. Wang, L. C. Hui, S. M. Yiu, G. Zhou, and R. Zhang, "F-DDIA: A framework for detecting data injection attacks in nonlinear cyber-physical systems," *Security and Communication Networks*, vol. 2017, p. 9602357, 2017.

[112] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *Ieee Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 6695779, 273–285, 2013.

[113] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for internet of things-based energy internet," *Future Generation Computer Systems*, vol. 93, pp. 849–859, 2019.

[114] Y. Xiang, L. Wang, and Y. Zhang, "Adequacy evaluation of electric power grids considering substation cyber vulnerabilities," *International Journal of Electrical Power and Energy Systems*, vol. 96, pp. 368–379, 2018.

[115] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, T. Cruz, and L. Lev, "From detecting cyber-attacks to mitigating risk within a hybrid environment," *Ieee Systems Journal*, vol. 13, no. 1, pp. 8352138, 424–435, 2019.

[116] A. Sharma, G. Rathee, R. Kumar, H. Saini, V. Vijaykumar, Y. Nam, and N. Chilamkurti, "A secure, energy-and sla-efficient (sese) e-healthcare framework for quickest data transmission using cyber-physical system," *Sensors*, vol. 19, no. 9, p. 2119, 2019.

[117] H. Yuan and Y. Xia, "Resilient strategy design for cyber-physical system under dos attack over a multi-channel framework," *Information Sciences*, vol. 454, pp. 312–327, 2018.

[118] S. Bezzaoucha, H. Voos, and M. Darouach, "Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems," *European Journal of Control*, 2018.

[119] Y. C. Sun and G. H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *International Journal of Robust and Nonlinear Control*, vol. 29, no. 14, pp. 4797–4811, 2019.

[120] H. Brown III, "Spcta: An analytical framework for analyzing cyber threats by non-state actors," in *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, pp. 135–158, IGI Global, 2019.

[121] D. Young, J. Lopez Jr, M. Rice, B. Ramsey, and R. McTasney, "A framework for incorporating insurance in critical infrastructure cyber risk strategies," *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 43–57, 2016.

[122] B. W. Wirtz and J. C. Weyerer, "Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats," *International Journal of Public Administration*, vol. 40, no. 13, pp. 1085–1100, 2017.

[123] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transportation Research Part A: Policy and Practice*, vol. 124, pp. 523–536, 2019.

[124] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient internet of things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260–13283, 2019.

[125] R. Sahay, W. Meng, D. A. Sepúlveda Estay, C. D. Jensen, and M. B. Barfod, "Cybership-iot: A dynamic and adaptive sdn-based security policy enforcement framework for ships," *Elsevier*, vol. 100, pp. 736–750, 2019.

[126] Y. Li, X. Liu, and L. Peng, "An event-triggered fault detection approach in cyber-physical systems with sensor nonlinearities and deception attacks," *Electronics (basel)*, 2018.

[127] M. Wang and B. Xu, "Observer-based guaranteed cost control of cyber-physical systems under dos jamming attacks," *European Journal of Control*, vol. 48, pp. 21–29, 2019.

[128] Y. C. Sun and G. H. Yang, "Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks," *Journal of the Franklin Institute*, vol. 355, no. 13, pp. 5613–5631, 2018.

[129] Y. G. Li and G. H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Information Sciences*, vol. 481, pp. 474–490, 2019.

[130] H. S. Lallie, K. Debattista, and J. Bal, "Evaluating practitioner cyber-security attack graph configuration preferences," *Computers and Security*, vol. 79, pp. 117–131, 2018.

[131] W. Zhang, Z. Wang, Y. Liu, D. Ding, and F. E. Alsaadi, "Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 1, pp. 53–67, 2018.

[132] P. Nespoli, D. Papamartzivanos, F. Goacutemez Maacutermol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *Ieee Communications Surveys and Tutorials*, vol. 20, no. 2, pp. 1361–96, 1361–1396, 2018.

[133] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, "Towards a framework for assuring cyber physical system security," *International Journal of Security and Its Applications*, vol. 9, no. 3, pp. 25–40, 2015.

[134] R. Kozik, M. Choraś, and J. Keller, "Balanced efficient lifelong learning (b-ella) for cyber attack detection," *Journal of Universal Computer Science*, vol. 25, no. 1, pp. 2–15, 2019.

[135] X. Fang, M. Xu, S. Xu, and P. Zhao, "A deep learning framework for predicting cyber attacks rates," *Eurasip Journal on Information Security*, vol. 2019, no. 1, p. 5, 2019.

[136] M. H. Khouzani, Z. Liu, and P. Malacaria, "Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs," *European Journal of Operational Research*, vol. 278, no. 3, pp. 894–903, 2019.

[137] Z. Zhan, M. Xu, and S. Xu, "Characterizing honeypot-captured cyber attacks: Statistical framework and case study," *Ieee Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 6587320, 1775–1789, 2013.