International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 1860-1874
http://www.ijcesen.com

ISSN: 2149-9144

Copyright © IJCESEN

Research Article

A National Cyber Risk Aggregation Framework: Why Micro-Security Metrics Fail at Macro Scale

Sairamesh Konidala*

Visvesvaraya Technological University, Bangalore, India
* **Corresponding Author Email:** sairameshkoni@gmail.com - **ORCID:** 0009-0004-6823-9410

Article Info:

DOI: 10.22399/ijcesen.5551
Received : 28 January 2025
Revised : 28 March 2025
Accepted : 30 March 2025

Keywords

Systemic cyber risk;
National cyber resilience;
Risk aggregation;
Critical infrastructure interdependence;
Security metrics

Abstract:

Macro-scale cyber risk is often inferred from micro-scale security metrics, including vulnerability severity scores, exploitability estimates, and enterprise attack-graph measures. This review assesses why micro-security measures do not necessarily remain valid when scaled to national-level risk assessment and develops the foundation for a national cyber-risk aggregation framework. Peer-reviewed journal articles and academic books on vulnerability scoring, exploit prediction, attack-graph analytics, cyber interdependence, cyber insurance, cyber resilience, and systemic cyber risk were critically evaluated. A literature-derived evidence map of 17 representative studies was coded using four analytical dimensions: analytical scale, dependency representation, validation strategy, and macro-readiness. The review finds that local observables remain most useful for bounded technical triage, while all vulnerability-scale studies reviewed lacked explicit dependency representation and all organization-scale attack-graph studies remained non-macro-ready without a cross-sector dependency layer. Macro-oriented studies have increasingly addressed contagion, tail dependence, and critical-function disruption, but they continue to rely more heavily on simulation and conceptual modeling than on well-observed national data. The evidence supports a multilayered approach in which local technical observables are translated through organizational, sectoral, and national dependency models before national impact is inferred. This review concludes that national cyber risk is an emergent construct of interdependent socio-technical systems, rather than a simple additive function of micro-level security measures. Future research should prioritize concentration-sensitive aggregation, resilience-oriented inference, explicit uncertainty treatment, and public-private evidence infrastructures for systemic calibration.

1. Introduction

For decades, cyber risk has been measured using artifacts designed for local use: vulnerability scores, estimates of exploitability, host-exposure indices, attack-path summaries, and measures of control-effectiveness. Such artifacts are operational since patch queues, segmentation policies, and security budgets need to be assigned to the level of certain assets, services and organizations. However, a national cyber-risk posture cannot be derived through simple aggregation of local scores. Interdependence between critical infrastructures, correlated software monocultures, supply-chain concentration, shared service providers, synchronized defensive failure, and coherent adaptation to points of vulnerability, are some of the factors that form national exposure. A scale that works well to prioritize a vulnerability in one company may thus not work when it is elevated to that of a national risk indicator [1]–[4].

It is not a semantic scale problem. The theory of information-security investment has historically shown that the marginal value of defensive spending is a factor of uncertainty, expected loss and risk transfer organization versus unadulterated technical severity [1]. It is also established in the economics literature that there are externalities in information security: when the costs of protection leak into other organizations, organizations will tend to underinvest, and decentralized decision-making will not be sufficient to produce socially efficient outcomes [2], [3]. As soon as those externalities are linked to infrastructures that provide electricity, finance, logistics, telecommunications, healthcare, and water, cyber

risk becomes a system performance stress issue as opposed to a technical weakness issue [4], [5].

This has been long since seen in the study of interdependence in infrastructure, before the emergence of cyber risk aggregation into a policy concern issue. Physical, cyber, geographic and logical connections among interdependent infrastructures can cause the failure of the infrastructure and the subsequent disruption can spread nonlinearly across sectors [4]. These seemingly minor disturbances at the node level in networked systems may result in a sudden systemic collapse when there are dense dependency ties or dependency link concentration [6]. The same logic applies to contemporary digital infrastructures. The similarities between cloud providers, identity providers, software repositories, managed security providers, industrial control providers, and protocol dependencies all create pathways through which a localized cyber incident can escalate into broader service failure with economy-wide consequences. Topology, concentration, substitutability, recovery coupling and timing are thus national exposure and none of which can be observed in a single vulnerability score.

The research field has thus altered its focus of limited security measurements to those of cyber resilience, systemic loss and insurability. The same issues of catastrophe modeling, critical-infrastructure resilience analysis, systemic financial risk are structurally analogous problems in cyber policy on the national level today. An approximation of the severity of an incident can be made using the worst compromised host or the highest Common Vulnerability Scoring System (CVSS) value whichever it may be. Instead, one would be interested in the dependencies of assets and institutions, the possibility to share common-cause failures, the common distribution of losses and the interdependence of cyber events and critical services [5]–[9]. Research on cyber insurance has further increased the weight to this concern by showing that cyber risk is difficult to pool when the losses are highly correlated, underreported or due to the highly dynamic nature of attack patterns [7], [8]. The same problem is reflected in national cyber-risk aggregation, which has more severe consequences, in the form of increased public-safety and macroeconomic impact.

A persistent challenge is that micro-security metrics remain more operationally established and institutionally dominant in practice. Most institutional dashboards still concentrate on the number of the most severe vulnerabilities, patch-latency, intrusion-alerts, mean-time-to-detect, mean-time-to-recovery, control-maturity, or local-attack-surface. These metrics are usually justifiable internally in the case of prioritization of objectives with limited resources. However, the assumptions underlying these metrics do not hold at the macro level. First, they are likely to think that they can be separated: the scores of the weaknesses can be evaluated individually and summed or averaged. Second, they typically consider dependency on a limited scale, like an internal attack graph, as opposed to firms, sectors and infrastructures. Third, they seldom simulate common-cause exposure due to the similarities in technologies and suppliers. Fourth, they are not very concerned with strategic feedback since the targets of attacks are chosen depending on likely defender responses. Fifth, they seldom quantify uncertainty in a form that it can be utilized in the country decision support.

The implications are substantial. When national authorities are dependent on the sum of micro measures, cyber preparedness may get exaggerated in areas that have effective local controls that do not have systemic redundancy. On the other hand, risk may be exaggerated in cases where there is the presence of technical exposure and service continuity is high because of fallback capacity, segmentation or quick reconstitution. On the policy level, improper aggregation might result in distorting capital allocation, industry pricing of cyber-insurance, industry oversight, and investment in resilience-enabling infrastructure. It can also provide misdirection to exercise and incident planning by taking into consideration technical severity comparison to service criticality and network position [7]- [9].

It is necessary to have a stringent national structure, therefore, that links at least four layers: the micro layer of technical vulnerability and exploitability; the meso layer of organizational structure and reliance on the supply-chain; the sector layer of service interconnectedness and service substitutability; and the macro layer of national essential-function persistence. The scientific problem is to preserve the content of information of local security measurements and yet not to encounter the pseudo accuracy that arises when the heterogeneous quantities are summed, not using a causal aggregation model. This dilemma remains unresolved: the literature is rich in local measures and increasingly attentive to systemic thinking, yet still lacks frameworks that integrate the two within a coherent logic of national aggregation.

That gap is filled by the current review which critically discusses why micro-security metrics do not work when scaled up to macro levels and by formulating the conceptual framework of a national cyber risk aggregation framework. It concentrates on the technical form of current measures, the assumption of reliance of a given measure, the form

of uncertainty that these measures represent, and the degree to which they can make or inhibit national level inferences. The review also reveals tendencies of methods employed in the literature and comes up with quantitative evidence of representative studies and proposes a multilayer aggregation architecture that emphasizes on interdependence, concentration, common-cause exposure, service criticality, and resilience. The central claim is that national cyber risk should be modeled as a systemic coupling problem rather than as an arithmetic extension of vulnerability severity.

2. Literature Review

A persistent imbalance in the cyber-risk literature is the contrast between mature, operationally embedded local technical indicators and the relatively sparse development of macro-level aggregation models. This gap does not reflect a lack of analytical sophistication. Instead, it is more of a reflection of the reality that a number of measurement traditions were developed in order to make all sorts of decisions. Triage was developed on vulnerability scoring. Attack-graph analytics of enterprises and remediation were created. The theory of interdependent-security was constructed, based on strategic interaction. Insurance and systemic-risk models were built up into correlated-loss models. These traditions operate within distinct analytical discourses, which obscures why micro-security measures fail when applied at the national level. The failure is brought about not by the weakness of statistics but by a lack of match between the measurement object and decision object.

At the vulnerability level, there was focus on literature that focused on severity ranking and exploit prioritization. The primary hypothesis is that the local technical characteristics could be transformed to ordinal or quasi-cardinal indicators that could be utilized to make remediation choices. Special review of CVSS revealed that the standard is helpful but volatile in interpretation especially where various assessors give various ratings to the same vulnerability [10]. Other schemes like the Vulnerability Rating and Scoring System (VRSS) was suggested to overcome perceived drawbacks of CVSS weighting and sensitivity to context [11]. Subsequent empirical studies shifted away off of severity and explored the question of the utilization of highly scored vulnerabilities in the wild. A case-control study showed that severity and real-world exploitation are not interchangeable and indicators of exploit moderately transform priorities logic [12]. The Exploit Prediction Scoring System (EPSS) advanced this shift by estimating exploitation likelihood from observed data rather than relying primarily on expert-assigned severity [13].

This body of work enhanced the local decision support, but also indicated why it is hard to aggregate local scoring on a national scale. The scores of severity do not rely on the level of dependency of the entities or their ability to replace services or the possibilities of sharing infrastructures. The exploit-probability models too are asset or vulnerability-based. They enhance ranking in remediation queues, but do not give any indication of whether the exploitation of a particular flaw would cause a focused sector outage or a service outage spread across geographical locations. The national risk aggregation is thus not appropriate with the output variable. A more accurate micro-level estimate does not eliminate macro-level blind spots; it merely increases confidence in an indicator that remains inappropriate for national inference.

The second significant tradition has to do with attack-graph and enterprise risk models. Such techniques are an explicit demonstration of dependency, but typically in the context of an organizational or mission setting. Probabilistic attack-graph work was initially done to model the probability of compromise via multiple steps and generate an overall network security measure out of local exploit network relationships [15]. The latter was followed by the discovery of how to use the metrics of attack-graph to assess the tradeoffs in the cost-benefits of an enterprise configuration choice and its payback on security investment [14]. This scheme was generalized in subsequent chapters and monographs to metric suites and resilience-oriented variants such as k-zero day safety, the capability to withstand unknown vulnerabilities that are structurally diverse and path disruption [16], [17]. These contributions are still key since they added causal dependency to the measurement of security instead of considering vulnerabilities as independent variables.

However, the enterprise attack-graph models do not often address the issue of national aggregation. Attack-path dependencies are their dependencies between hosts, services, privileges and protections of a known architecture. Another type of dependencies, contingent on national risk, is cross-firm reliance on services, sector-level concentration, monoculture of the software, similarities of the providers, and recovery interference. A single enterprise attack graph might be valuable in quantifying the diffusion of a single compromise path in an internal network, but is not generally valuable in quantifying the diffusion of a single provider outage in hospitals, payment

systems, logistics operators and public communications. With local path measures which do not model these larger channels, an inaccurate approximation of national exposure will be obtained. In other words, dependency modeling is necessary but not sufficient; the scale of the dependency model must match the scale of the policy question.

This is a scale question that is raised by the interdependent security literature. The interdependent risk network security games and models revealed that the security decisions of one actor would influence the payoffs and exposures of other actors [18], [19]. These works changed the focus of efforts on isolated control performance towards equilibrium behavior with externalities. They also elaborated why voluntary investments can never be optimum even in situations where organizations act rationally in their interest. This is necessary on the national cyber risk as sector resilience will rely on distributed decisions on patching, segmentation, redundancy, cyber hygiene and incident disclosure. Provided that the decisions are interdependent, the country risk cannot be built with the local scores but the representation of the coupling mechanism must be analytical.

The interdependent-security models however, are stylized. They can provide a good theoretical knowledge of strategic complementarity, free riding, and contagion yet can be an abstraction of the technical and operational heterogeneity of real infrastructures. In turn, they find the cause as to why aggregation is a problem without necessarily giving an effective aggregation structure. The gap in the literature has been identified as one of the primary ones being the inability to bridge the gap between the technically detailed enterprise measurements and the economically reasonable network models.

A closer effort to deal with macro aggregation was in the literature on cyber-insurance and systemic-risk. The analysis of aggregate cyber-risk management in the Internet of Things (IoT) age indicated that the normal levels of technological exposure can cause disproportionate portfolio losses, and may fail the conventional diversification arguments [20], [21]. Associated insurance studies proved that the existence of model risk per se may turn into significantly distorted pricing and sensitivity calculations in case of cyber losses aggregated within insufficient dependence frameworks [22]. Insurance portfolio network-contagion model also pointed out that explicit connectivity and propagation assumption convert the procedure of losses [24]. These insights are highly relevant to national cyber risk because the state faces a portfolio problem: its vital services are collectively vulnerable to common software, service providers, and attack programs. This is no change of logic of aggregation but of the impact of error. The misspecification of the models used in national contexts does not only distort the premiums, but also preparedness, regulation and crisis coordination.

Systemic cyber-risk scholarship has thus focused on interdependence, concentration and critical-function continuity, instead of numbers of vulnerabilities. Nationally consequential cyber risk has been proposed as an issue where the disturbance propagates throughout socio-technical infrastructures and destabilizes the safety of the population, economic stability and ability to control the populace [23]. It is more a methodological orientation to resilience analysis and catastrophe modeling than the conventional vulnerability management. The critical chain of functions or services turns into the unit of analysis, and not the single technical flaw.

There are four tensions in the comparative literature. First, most models exhibit an inverse relationship between technical fidelity and systemic scope. High fidelity metrics in a local sense are not scalable; and systemic models are apt to lose technical detail. Second, severity rankings and probabilities are frequently used together, without a definite causal linkage. Third, practices of validation vary dramatically, with vulnerability models typically being tested on observed exploit or expert-labeled data, and macro models typically being analytically or simulated. Fourth, uncertainty is not treated in a consistent manner. Local scores imply accuracy but do not measure the uncertainty of dependence but systemic models are conscious of uncertainty and cannot be high-resolution.

Those tensions are the reason why micro-security measures are institutionally hegemonic to the macro constraints of these measures. They are simpler to work out, simpler to describe in operation, as well as simpler to update using scanning data. Macro models require data that is heterogeneous, knowledge of the sector, mapping of infrastructure and reasoning of scenarios under uncertainty. But the literature also shows that the micro-centric course of action can no longer suffice. Aggregation error is a first-order policy issue, rather than a nuisance of methodology, in the case of digital infrastructures that are centralized and mutually dependent.

A comparative contribution-level summary is provided in Table 1. The table indicates that the output variables of local metrics are mostly severity, the probability of exploit, the exposure of attack-path or enterprise risk, and macro-oriented studies focus on contagion, concentration, tail loss

and the impact of critical functions. A comparison of metric families, their dependency assumptions and their main way of failure under national aggregation is given in Table 2. As indicated in Figure 1, vulnerability and attack-graph families are the most common phenomenon in the historical literature and Figure 2 indicates that explicit dependency representation is only more likely to arise when the scale of analysis is no longer the individual vulnerability or enterprise.

The main implication of the reviewed literature is not that micro-security measurements are meaningless. At the level, which they were meant to serve, they cannot be dispensed with. The error is category error. The partial observables of national cyber risk are severity scores, exploit predictors and enterprise attack graphs, rather than being estimators of cyber risk. When they are read as national indicators, they immediately fail to represent the concentration, misrepresent common-cause exposure and lack systemic service implications, which is the case in the absence of dependency-sensitive aggregation frameworks.

3. Methodology

This review conducted a structured narrative synthesis of peer-reviewed journal articles and academic books related to the measurement of cyber risk, cyber resilience, interdependence of infrastructures and systemic cyber-loss aggregation. This was not to enumerate the publications on the security metrics, but to identify the traditions in methodology that would most likely have a bearing on the transition towards measuring micro-security to the national cyber-risk. As such, sources were chosen wherein at least one of the following criteria were met: a formal measure of technical exposure was put forward; interdependence between cyber factors or organizations was modeled; cyber loss or systemic impact was aggregated across portfolios or industries; or resilience and systemic impact were explicitly modeled as targets of analysis.

The review was structured around the keywords ‘cyber-risk aggregation,’ ‘systemic cyber risk,’ ‘security metrics,’ ‘vulnerability scoring,’ ‘exploit prediction,’ ‘attack graph,’ ‘interdependent security,’ ‘cyber insurance,’ ‘critical infrastructure interdependence,’ ‘cyber resilience,’ and ‘national cyber risk. The review covered literature published between 2001 and 2025, with particular emphasis on work published after 2010 as it showed the maturity of the vulnerability scoring criticism, the creation of the attack-graph metrics, and the recent transition to systemic and portfolio modeling. Peer-reviewed journal articles and academic books or book chapters were the only sources that were retained in the evidentiary core. Even powerful in practice, Web sites, industry white papers, preprints and grey literature were not part of the formal review corpus because it was necessary to ensure that the analysis was grounded in citable scholarship.

Greater emphasis was placed on the logic of measurement than on the volume of publications. A common analytical framework was therefore used to examine the studies across six variables: unit of analysis, dependency representation, primary output variable, validation strategy, uncertainty treatment, and macro-readiness. Unit of analysis was used to determine whether a study primarily focused on vulnerabilities, enterprise networks, supply chains, sectors, national critical infrastructures or insurance portfolios. Dependency representation captured whether the representation of exposure was independent, attack paths, strategic interaction or common technology or provider dependence, or cyber-physical service interdependence. The output variable was used to determine whether a study represented the output as impact, exploitability, enterprise compromise, recovery (resilience), systemic vulnerability or portfolio loss. The validation strategy was defined as expert scoring, empirical exploit data, simulation, case study, conceptual demonstration or portfolio risk-loss analysis. For macro-metrics, the definition of correctness was not predicting a future national loss. Instead, a macro-metric was deemed more valid if it captured the relevant dependence channel, could be benchmarked against incident, outage, recovery, insurance-loss or sector-disruption data (where available), provided reasonable rankings of essential-function disruption under scenario-based stress tests, and provided sensitivity to concentration, recovery and dependence measures. The qualitative variable uncertainty treatment captured whether a study mentioned variation, tail risk, reporting bias, learning/adaptation of adversaries or model risk. The macro-readiness variable was coded as conservative, and only applied to studies that could be used to inform aggregations for sectors and the nation while not changing the object of measurement.

This approach was chosen because past analyses of cyber risk assessment processes have invariably indicated that methodological heterogeneity as such is one of the fundamental impediments to comparison [25], [30]. Frameworks differ both in terms of assumptions, as well as the thing measured. An exploit prediction, a vulnerability measure, an attack-path measure, a FAIR-style loss measure, and a resilience measure are often thought to be in the same metric family, which, however, is

a misnomer, given that they address different causal questions. The literature can become more cumulative only when the measurement object is normalized explicitly across studies.

Technical tools are also in stark contrast between the reviewed studies. Expert judgment system, event labeling based on empirical research and statistical prediction based on CVE related data are typical of studies that concentrate on the issue of vulnerability [10] -[13], [31]. Enterprise network analysis is based on attack graphs, Bayesian reasoning, path enumeration and mission- or cost-based scenario analysis [14]-[17], [26]. Instead of pure adversarial probability introduced by systems methods, dependency networks, and consequence-oriented indicators, resilience-oriented studies introduce them [28], [29]. The application of contagion processes, dependence structures, market or industry simulation and tail sensitive risk measurement is more common to portfolio and systemic studies [20] -[24]. These technical variations were not assumed to be noise; instead, they were seen as a testament to the fact that national aggregation needs a layered model, which can integrate heterogeneous data, causal mechanisms instead of choosing a single preferred local measure.

A final set of 17 representative studies was used to create a structured evidence map spanning vulnerability scoring, exploit prediction, enterprise attack-graph metrics, interdependent-security models, cyber-insurance aggregation, resilience measurement, and systemic cyber-risk framing. To reduce the risk of selective citation, the final corpus was documented by analytical unit, metric family, dependency channel, output variable, and limitation for national aggregation, as shown in Table 1. The studies were not treated as an exhaustive bibliometric sample; rather, they were selected as a structured, theory-building evidence set representing the principal methodological traditions needed to explain why micro-security metrics fail under national-scale interpretation. This coding process provided the basis for the descriptive tables and figures presented in the manuscript. Because each coded entry is linked to a peer-reviewed article or academic book chapter, the evidence map remains transparent and reproducible within the stated scope of the review.

This design has two design caveats. To begin with, it is important to recognize that macro-readiness is an evaluation of transferability to national aggregation, and not that a particular study was designed to be used in national policy. Second, the interpretation of quantitative summaries made on the basis of coded literature is to be interpreted in a descriptive way, but not in an inferential way. They should reflect structural inclinations of the literature reviewed, e.g. emphasis of evidence at certain scales or reliance on certain validation methods. They do not aim at estimating the actual distribution of all cyber-risk publications.

The review methodological conclusion is thus two-fold. The existing literature may be considered to be in a stack of measurements rather than as an alternative to each other. Further, whether or not a national aggregation framework can be linked across scale without uniting different constructs into a single score that is misleading determines the viability of the framework. This reasoning guided the discussion of the results and the presentation map proposed in the discussion.

4. Discussion

The coded literature shows that the central problem in national cyber-risk aggregation is not the absence of metrics, but the mistaken assumption that the same metrics remain valid across different scales. Within the 17 studies included in the evidence map, 52.9% of the studies would be described as micro-focused i.e. the output would be most aptly considered at vulnerability, system, site or enterprise level and 47.1% of the studies would be macro-ready i.e. the output would directly address sector, supply-chain, portfolio or systemic dependence. This is a close balance that is misleading. The work in the latest period is much concentrated in macro-ready. Only a small proportion of the studies published before 2021 were macro-ready; the percentage shot up significantly after 2021. This inflection is captured by figure 3. The literature has thus shifted to systemic framing, though in operation practice and most institutional dashboards are still stuck in the older metric families.

The initial substantive pattern is an issue of contrasting the technical dependency and systemic dependency. Attack-graph work is a model on many micro studies that model dependency. Explicit path dependency was used in the coded sample of all the organization-level attack-graph studies. Nevertheless, there are still models, which are limited to enterprise architecture. They demonstrate the local compromise advance within a network or mission setting, and not the spread of disruptions across shared cloud tenancy, software monoculture, managed services, vendor ecosystem around an industry, or service chains nationwide. This is an important difference. This indicates that the mere presence of dependency modeling does not imply macro-level suitability. Dependency has to be expressed on the level of the policy question. Table 3 indicates that the empirical evidence base is

saturated with vulnerability and organization level studies yet do not provide many direct leverage points of national aggregation because of the local dependency channel, rather than systemic dependence channels.

The second one is the low correlation between severity based measurement and national consequence. Both cyber resilience literature and critical-infrastructure modeling literature repeatedly note that the consequence of service is a factor of redundancy, substitutability, temporal coupling, and restoration channels and not necessarily due to technical severity alone [32], [33], [36], [37]. A technically modest incident affecting a highly central service provider can therefore have greater national consequences than a major compromise at a marginal asset. On the other hand, technically severe incident may be confined to a nation in the presence of service rerouting, manual fallback and organizational slack. This is the primary reason why micro-security indicators are not scales to macro-level: they are intensity measures of local vulnerability, but the cyber risk to the country is a consequence measure which is mediated by the network structure.

The third pattern relates to common-cause exposure and concentration. Recent studies into cyber-risk assessment, resilience management and insurance show that systemic losses arise when a large number of entities are exposed to the same technological or organisational or shared service infrastructure [34], [37], [38]. This can be classified into at least two types. Structural common-cause exposure refers to common technical infrastructures and platforms, such as common software libraries, cloud computing platforms, identity management systems, industrial protocols, dependency on DNS, managed security services and leading hardware/operational technology vendors. Functional common-cause exposure is based on shared services, including power, telecommunications, payment processing, supply chain, water, emergency communications and other utilities that are necessary for continuity across industry segments. Local metrics can indicate these exposures as "repetition". At a national level, repetition is not accidental; it may be an indicator of concentration. Thousands of local vulnerabilities in strategically critical systems don't represent thousands of risks, but could represent a common event. Sum of local counts can therefore overestimate tail risk.

A fourth is validation asymmetry. The coded corpus shows that micro studies have a higher likelihood of being empirically validated especially in the vulnerability scoring and exploit prediction domain, and whereas macro-ready studies rely more heavily on conceptual argument, simulation, or portfolio modeling than on direct empirical validation. This imbalance is shown in figure 4. This difference can be utilized to justify why micro metrics can be held by the institutional legitimacy. They may be associated with observable instances of exploits, scanner results, expert tags or testbeds. The national aggregation models, their part, have limited incident data, selective reporting and proprietary exposure maps, and unpredictable adversarial behavior. It is irrelevant that rich macro data are not available; it alters the shape of defensible inference. Models developed nationally must thus be structured to work even in the face of structured uncertainty as opposed to waiting until the ideal data sets come about.

A fifth important finding concerns analytical scale. Table 3 shows that there are no macro-readiness regardless of the operational maturity of the vulnerability in the sample of the vulnerability studies. Organization level studies provide the structure with the help of attack graphs and are still locally bounded. Portfolio/market and national/systemic studies are designed to be macro-ready, although they are not so prevalent or standardized. Supply-chain research is between the two because it can be identified but is interdependence between organizational divisions [35]. This middle-ground is of special interest to national frameworks. It can project the circumstances of local control onto the forms of sectoral dependence without having to assume that the risk of the populace is represented by a single measure of an enterprise.

These observations indicate that there are multiple layers to cyber aggregation. The output of national cyber risk should be the four transformations coupled with it. Initially, local technical observables have to be estimated: the severity of vulnerability, the exploitability, the exposure, credential privilege, service hardening, and recovery capacity. Second, observables have to be mapped into service dependencies within an organization, such as cloud, identity, software, logistics, and operational-technology dependency. Third, the concentration and substitutability on the sector level should be determined: the number of critical providers with the same dependencies, the presence of alternatives, and the ability to quickly switch. Fourth, essential-function disruption, length and social or economic effects should be used to conceptualize national consequence. The literature repeatedly supports individual segments of this transformation chain, but rarely the chain as a whole [32]–[39].

The suggested form of this transformation is shown in Table 4. The table confirms that there are five

failure modes which repeat when local metrics are scaled to macro scale in the absence of causal bridge: false independence, false cardinality, false comparability, false stability and false completeness. False independence is the addition of local results in the same fashion loses are independent. False Cardinality is the case when the categories of severity, which are ordinarily interval data, are averaged. False comparability is a scenario in which the different sectors are compared with measures that do not consider criticality of services and resilience capacity. False stability occurs when the assumption of exploiting the static scores as exposure is done even in the presence of the adversarial adaptation and shifting dependencies. False completeness occurs when seemingly technical inadequacies are theorized as the national risk at large when recovery, substitution and concentration is not measured.

The implications of the framework are simple. Micro-security metrics should not be discarded within a national cyber-risk aggregation architecture; rather, their use should be disciplined by it. The inclusion of local metrics into the framework can only be achieved by being re-expressed using dependency and consequence models. This means that there exist hierarchical architecture in which micro observables are kept at the bottom but processed in network aware layers. This type of design can be used with resilience-based risk governance since the same local data can be utilized in both enterprise activities and national preparedness, as long as the aggregation model is clear concerning the concentration, substitution, as well as critical-function impact [36], [37].

The literature proposes as well that the resilience metrics should be regarded as equal to the compromise metrics. Studies of cyber-physical systems are especially valuable because minimum-effort attack strategies relate adversarial effort to operational pathways rather than to vulnerability severity alone [39]. Interdependent infrastructures surveys also reveal that the propagation of failures also lies on the restoration logic, control coupling and operational redundancy [32], [33]. National aggregation thus necessitates two concurrent perspectives which are: one that talks about the diffusion of attacks and another that talks about absorption, degradation and recovery of services. Micro-security metrics tend to only shed light on the former.

Finally, the reviewed evidence shows that model uncertainty should be made explicit. Systemic and insurance studies have demonstrated that the assumption of dependence can take over aggregate loss estimates [22], [24], [38]. A national system that is constructed on local scores, which are accurate, but with opaque assumptions of aggregation would thus give an illusion of analytical rigor. The uncertainty ought to be considered as a first-class output. Scenario ranges, dependency bounds, concentration stress tests, and recovery sensitivity analysis are not optional refinements, but are the processes by which national cyber risk can be decision-usable.

The interpretation that has come out is neither anti-metric nor anti-operational. It is a position scale-corrective. Vulnerability scores, exploit predictions and enterprise attack graphs are still tools that are needed. It is not the fact that these instruments can be added, averaged, or weighted to a plausible national risk index, in the absence of a dependency-conscious model of the consequence of service. The cyber risk within the country is on the rise. Any framework that fails to put into consideration emergence will not quantify emergence.

5. Future Directions

Future research should move beyond the search for a universally superior local measure and instead develop scale-linking architectures. According to the literature, the unresolved issue of greatest urgency is not that a higher number of vulnerability scores are produced but that defendable rules of transformation that project local technical observables into service-level and national-level consequence. These are rules which must be causal, stratified and uncertain. It is a weak national framework so long as it continues to build on the foundation of public consequence based on the technical intensity, without modelling the concentration and dependence on services.

Multilayer dependency modeling is a first-priority. The available literature is inclined to concentrate on only one dependency category: the attack routes within a company, the strategic interdependence between companies, the dependence between portfolios in insurance or the cyber-physical dependence in infrastructures. These layers need to be united in the process of national aggregation. There is a need to conduct research on models that allow the representation of host-to-service, service-to-provider, provider-to-sector and sector-to-essential-function dependence in a single coherent model. It is not yet excluded that the methods will be based on graphs, but the methods of the future must incorporate typed edges, and recovery constraints and weights of concentration along with the connectivity. Factor graphs, dynamic Bayesian networks, and hybrid network-flow models may be especially useful in those cases, when the dependence between layers is heterogeneous.

Concentration sensitive exposure measurement is a second priority. National cyber exposure increases when many critical organizations rely on the same software, provider, protocol, or identity service. This type of duplicating is normally smoothed by the existing micro metrics to local discoveries that are recurring. The way forward in terms of the future work should therefore come up with concentration operators which transform the repetitive technical observations into the common-cause national stress indicators. These types of operators must take into consideration market share, criticalness of sector, substitutability and geographic coupling. A weakness in an ordinary, and substitutable element must not receive such treatment as a vital provider of operations with a profound involvement.

The third priority is to include resilience as a quantifiable equivalent of compromise. Cyber-resilience reviews argue that anticipation, absorption, recovery, and adaptation should be measured alongside prevention and detection [40], [41]. Fallback capacity, recovery time distributions, manual workarounds, spare operational capability, as well as, restoration interdependence should thus be variables in national cyber frameworks. The methods that can be used to correlate local technical compromise with degradation and reconstitution of crucial functions are required especially in research. These models would help bridge the longstanding gap between cyber measurement and continuity planning;

Uncertainty representation is a fourth priority. The national models will continue to be biased in their operations, and partial disclosure, altering opponents, and turbulent dependence networks. Future frameworks should represent uncertainty explicitly rather than obscuring these limitations. As standard output should be treated scenario envelopes, parameter range, stress-testing bands and model-structure sensitivity. This would balance aggregation of national cyber-risk exposure with well-developed catastrophe and systemic-risk analysis whereby the decision-makers would not get a unitary, unconfidence-based figure.

A fifth priority is to improve the evidence infrastructure. Cyber risk study is hampered by poor-quality data streams of exposure, dependency, outage, recovery and loss [30], [38]. Future national frameworks require well-observed data streams that can be used to calibrate dependency-sensitive models, such as anonymous cyber-insurance claims, privacy-preserving incident and outage reporting, sector-specific distributions of recovery time, concentration maps of providers, software and cloud dependency registers, global routing or traffic telemetry, and continuity logs of critical services. These should be released through secure public-private data streams such that competitive, security and privacy issues are preserved, but systemic calibration can take place. This might be helped with data trusts, privacy-preserving data-pooling, regulatory safe harbours, reporting taxonomies etc. In the absence of such data streams, national frameworks may be well-conceived but poorly calibrated and unverified.

A sixth priority concerns adversarial adaptation. Many aggregation models still treat risk as the result of exogenous shocks. The contrast to cyber risk is that the enemies change the target to areas of concentration, areas that are underdefended and new areas which have become valuable. There should thus be some strategic feedback in national frameworks in particular cases when defensive interventions change attractiveness of targets. This means that it has a greater role of game-theoretic and adaptive simulation techniques associated with real dependence maps compared to single payoff model.

A seventh priority is essential-function validation. Future studies ought to pit national aggregation frameworks to scenarios of multi-sector service-disruption, as opposed to just exploit or compromise datasets. Validation targets are continuity of payment, delivery of care, dispatch of energy, telecommunications, logistics, communications with safety of the populace, water operations. A framework with accurate predictive ability of local compromise, but a lack of the credibility of rank among the essential-function disruption, cannot be used nationally.

The wide line of direction is evident. The next step of cyber measurement should be to go beyond the enumeration of weaknesses to modeling nationally important dependency structures in the face of uncertainty. The scientific advantage is to make the heterogeneous local observables into the public-risk intelligence without destroying the process through which the macro consequences are created.

Table 1. *Comparative review of representative studies on cyber-risk measurement and aggregation*

Ref.	Study	Primary analytical unit	Metric family	Dependency channel modeled	Output variable	Principal limitation for national aggregation
[10]	Holm &	Vulnerability	Vulnerability	None	Severity	No service or cross-

	Afridi (2015)		scoring		calibration	entity dependence
[11]	Liu & Zhang (2011)	Vulnerability	Vulnerability scoring	None	Severity score	Ordinal score not suitable for systemic consequence
[12]	Allodi & Massacci (2014)	Vulnerability	Exploit empirics	None	Exploit likelihood	Improves prioritization but not cross-sector impact
[13]	Jacobs et al. (2021)	Vulnerability	ML vulnerability prediction	None	Exploit probability	Asset-centered output remains nationally incomplete
[14]	Noel et al. (2010)	Organization	Attack-graph metric	Internal attack paths	Risk/ROI metric	Enterprise boundary excludes sector contagion
[15]	Wang et al. (2008)	Organization	Attack-graph metric	Internal attack paths	Probabilistic security metric	No provider or supply-chain concentration layer
[16]	Noel & Jajodia (2017)	Organization	Attack-graph metric suite	Internal attack paths	Composite network metric	Path dependence is local, not national
[17]	Wang et al. (2017)	Organization	Attack-graph resilience	Unknown-vulnerability paths	k-zero day safety	Structural diversity is not mapped to essential functions
[18]	Hofmann & Ramaj (2011)	Network/Sector	Interdependent risk network	Cross-firm contagion	Systemic exposure pattern	Technically abstract, limited operational calibration
[19]	Laszka et al. (2014)	Network/Sector	Interdependent security game	Strategic interdependence	Equilibrium risk	Strategic insight exceeds direct measurement output
[20]	Pal et al. (2021)	Portfolio/Market	Insurance aggregation	IoT common-cause exposure	Aggregate tail risk	Limited direct mapping to national service continuity
[22]	Peters et al. (2023)	Portfolio/Market	Insurance model risk	Tail dependence/model uncertainty	Premium sensitivity	Strong aggregation insight but insurer-oriented output
[23]	Setola (2023)	National/Systemic	Systemic cyber risk	Critical-infrastructure interdependence	Systemic risk framing	Requires richer exposure data for operational deployment
[24]	Hillairet et al. (2022)	Portfolio/Market	Insurance contagion	Network contagion	Contagion-adjusted loss	Loss orientation needs coupling to essential-function metrics

Table 2. *Metric families and their failure modes under macro-scale interpretation*

Metric family	Typical data inputs	Native decision context	Strengths	Failure mode at macro scale
Vulnerability scoring	CVE attributes, expert-defined factors	Patch triage	Fast, standardized, comparable within local workflows	Treats dependencies as absent; invites false cardinality
Exploit prediction	Historical exploit evidence, vulnerability metadata	Prioritization of remediation queues	More behaviorally grounded than severity alone	Still asset-centered; weak on service consequence
Attack-graph metrics	Network topology, vulnerabilities, privileges, firewall rules	Enterprise exposure reduction	Captures multistep causality inside bounded systems	Usually excludes cross-firm, sector, and provider concentration
Interdependent security games	Strategic actors, incentives,	Policy/economic reasoning	Captures externalities and	Often too stylized for operational

	spillovers		underinvestment logic	aggregation
Cyber-insurance aggregation	Portfolio exposure, dependence assumptions, loss models	Capital allocation and pricing	Explicit about correlation and tail risk	Needs translation from loss portfolios to national functions
Cyber-resilience metrics	Recovery, absorption, adaptation, continuity variables	Operational resilience and continuity	Closer to public consequence and essential services	Often lacks tight linkage to technical attack observables
Systemic cyber-risk frameworks	Multi-sector dependency maps, concentration, common causes	National preparedness and supervision	Scale-consistent with policy objectives	Data scarcity and calibration remain limiting factors

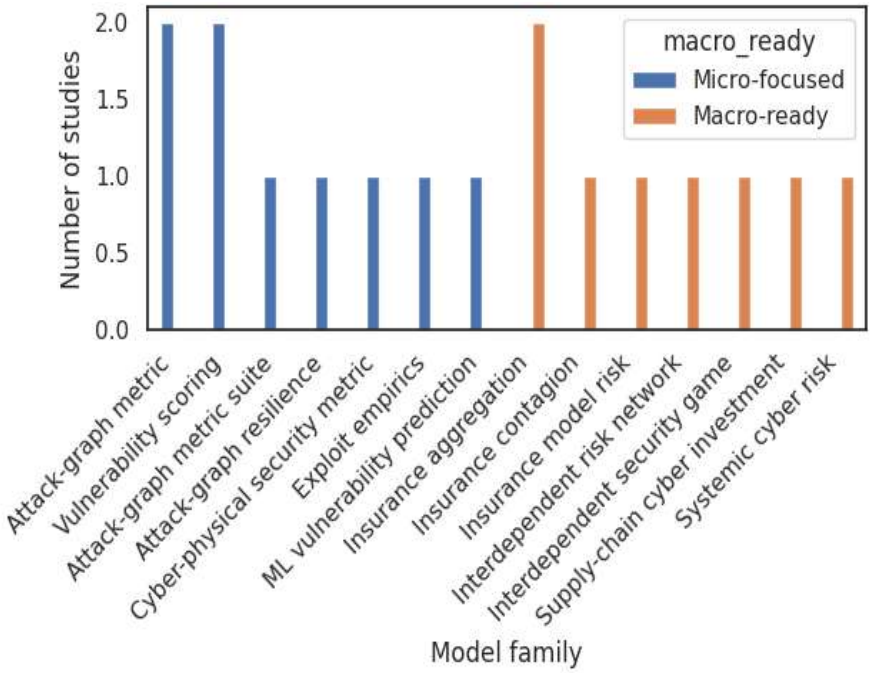


Figure 1. *Distribution of model families by study orientation*

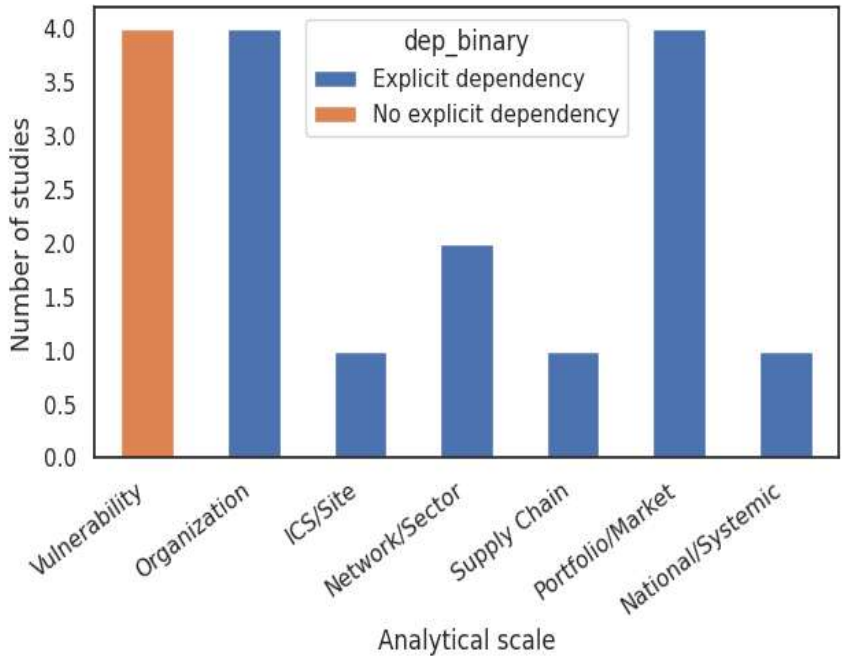


Figure 2. *Explicit dependency treatment across analytical scales*

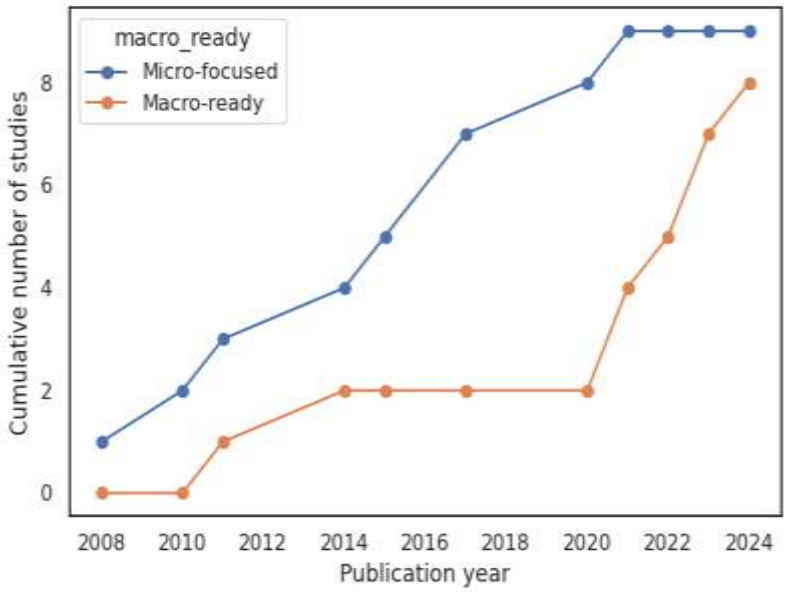


Figure 3. *Cumulative shift from micro-focused to macro-ready studies*

Table 3. *Descriptive summary of the coded evidence map by analytical scale*

Analytical scale	Number of studies	Studies with explicit dependency	Macro-ready studies	Empirically validated studies	Median publication year
Vulnerability	4	0	0	3	2014.5
Organization	4	4	0	0	2013.5
ICS/Site	1	1	0	1	2020.0
Network/Sector	2	2	2	0	2012.5
Supply Chain	1	1	1	0	2024.0
Portfolio/Market	4	4	4	0	2021.5
National/Systemic	1	1	1	0	2023.0

Table 4. *Proposed national cyber-risk aggregation logic and recurrent failure modes*

Aggregation layer	Core inputs	Required transformation	Common error when omitted	National relevance
Micro-technical layer	Severity, exploitability, exposure, privilege, control state	Convert local findings into service-relevant technical observables	False cardinality: ordinal scores treated as additive magnitudes	Necessary but insufficient
Organizational service layer	Internal architecture, identity, cloud, OT/IT linkage, recovery procedures	Map technical states to mission/service degradation	False completeness: compromise treated as consequence	Connects security to operations
Sector dependence layer	Supplier commonality, provider concentration, substitution capacity, timing	Estimate correlated disruption across organizations	False independence: duplicated local risk treated as uncorrelated	Reveals common-cause national exposure
Essential-function layer	Service criticality, population served, fallback capacity, restoration coupling	Translate sectoral disruption into public consequence	False comparability: equal treatment of unequal functions	Aligns metrics with public policy
Uncertainty layer	Parameter ranges, model ambiguity, reporting gaps, adversarial adaptation	Produce scenario bands and sensitivity outputs	False stability: point estimates mistaken for robust truths	Supports defensible decision-making

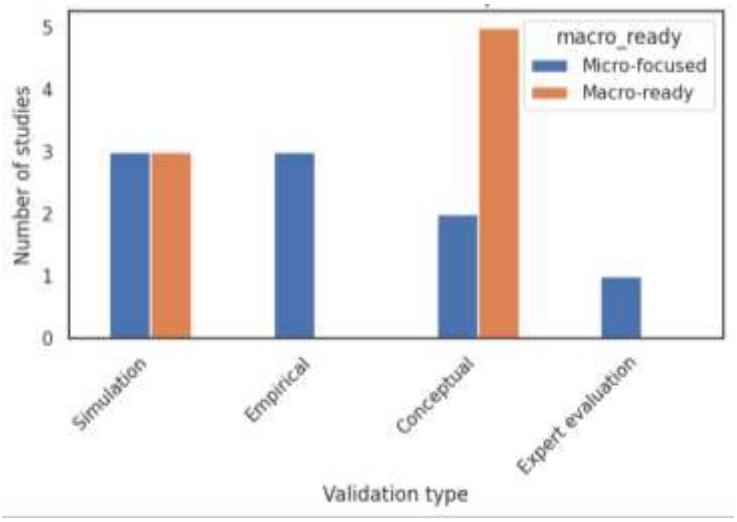


Figure 4. *Validation evidence across study orientations*

6. Conclusions

The reviewed literature shows that national cyber risk cannot be inferred through mechanical aggregation of micro-security metrics. The scores on vulnerability, exploit predictors and enterprise attack-graph scores are valuable as they are operational descriptions of the local technical conditions. They start failing when they are considered to be measures of systemic consequence already. At the national level, the sources of cyber risk are interdependence, concentration, common-cause exposure, service criticality and recovery coupling. The processes bring the disruption of local technical states to the macro level that cannot be summed, averaged, or weighted.

The review also reveals a shift from micro to macro studies in cyber insurance, critical-infrastructure dependency and cyber resilience. However, a full connection from micro to macro is yet to be realised. What is needed is a multilayer aggregation system in which local technical information is retained but reinterpreted through organizational, sectoral, and national dependency models. Such a framework should distinguish technical intensity from public consequence, structural common-cause exposure from functional service dependence, compromise from resilience, and point estimates from uncertainty-sensitive scenario outputs. Its use will also require new national evidence systems, such as anonymised loss data, outage-and-recovery data, provider-concentration maps, dependency registries and privacy-protecting telemetry.

The implication on the ground is that the national cyber preparedness cannot be enhanced only by honing local measures. Improved severity scores and exploit forecasts are beneficial, but they do not in themselves solve the macro-level problem. The way forward lies in building scale-consistent models to tie together what is measured at the local level with what is important at the national level: continuity of crucial functions in adverse stress. The field should then not only take into account the prediction accuracy of future cyber-risk measures at a local scale, but also whether they preserve the causal meaning at the scales. A measure that cannot carry its causal meaning across scales should not be used as the basis for national policy.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457.

[2] Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613.

[3] Kunreuther, H., & Heal, G. (2003). Interdependent security. Journal of Risk and Uncertainty, 26(2–3), 231–249.

[4] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25.

[5] Dueñas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. Structural Safety, 31(2), 157–167.

[6] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025–1028.

[7] Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy, 2(1), 53–63.

[8] Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474–491.

[9] Welburn, J. W., & Strong, A. (2022). Systemic cyber risk for national critical functions. Risk Analysis, 42(8), 1606–1622.

[10] Holm, H., & Afridi, K. K. (2015). An expert-based investigation of the Common Vulnerability Scoring System. Computers & Security, 53, 18–30.

[11] Liu, Y., & Zhang, Y. (2011). VRSS: A new system for rating and scoring vulnerabilities. Computer Communications, 34(3), 264–273.

[12] Allodi, L., & Massacci, F. (2014). Comparing vulnerability severity and exploits using case-control studies. ACM Transactions on Information and System Security, 17(1), 1–20.

[13] Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit Prediction Scoring System (EPSS). Digital Threats: Research and Practice, 2(3), Article 20, 1–17.

[14] Noel, S., Jajodia, S., Wang, L., & Singhal, A. (2010). Measuring security risk of networks using attack graphs. International Journal of Next-Generation Computing, 1(1), 135–147.

[15] Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric. In V. Atluri (Ed.), Data and Applications Security XXII (pp. 283–296). Springer.

[16] Noel, S., & Jajodia, S. (2017). A suite of metrics for network attack graph analytics. In L. Wang & S. Jajodia (Eds.), Network Security Metrics (pp. 141–176). Springer.

[17] Wang, L., Jajodia, S., Singhal, A., Cheng, P., & Noel, S. (2017). k-zero day safety: Evaluating the resilience of networks against unknown attacks. In L. Wang & S. Jajodia (Eds.), Network Security Metrics (pp. 75–93). Springer.

[18] Hofmann, A., & Ramaj, R. (2011). Interdependent risk networks: The threat of cyber attack. International Journal of Management and Decision Making, 11(5–6), 312–323.

[19] Laszka, A., Felegyhazi, M., & Buttyan, L. (2014). A survey of interdependent information security games. ACM Computing Surveys, 47(2), Article 23, 1–38.

[20] Pal, R., Huang, Z., Yin, X., Lototsky, S., De, S., Tarkoma, S., Crowcroft, J., Liu, M., Sastry, N., & Nag, B. (2021). Aggregate cyber-risk management in the IoT age: Cautionary statistics for (re)insurers and likes. IEEE Internet of Things Journal, 8(9), 7360–7371.

[21] Pal, R., Huang, Z., Lototsky, S., Yin, X., Crowcroft, J., Liu, M., De, S., Sastry, N., & Nag, B. (2021). Will catastrophic cyber-risk aggregation thrive in the IoT age? A cautionary economics tale for (re-)insurers and likes. ACM Transactions on Management Information Systems, 12(2), Article 17, 1–28.

[22] Peters, G. W., Shevchenko, P. V., Lin, Z., Wüthrich, M. V., & Zhang, Y. (2023). Cyber loss model risk translates to premium mispricing and risk sensitivity. Geneva Papers on Risk and Insurance: Issues and Practice, 48(2), 372–433.

[23] Setola, R. (2023). Systemic cyber risk. International Journal of Critical Infrastructure Protection, 43, 100652.

[24] Hillairet, C., Lopez, O., d'Oultremont, M., & Spoorenberg, T. (2022). Cyber-contagion model with network structure applied to insurance. Insurance: Mathematics and Economics, 107, 88–101.

[25] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27.

[26] Singhal, A., & Ou, X. (2017). Security risk analysis of enterprise networks using probabilistic attack graphs. In L. Wang & S. Jajodia (Eds.), Network Security Metrics (pp. 53–73). Springer.

[27] Hubbard, D. W., & Seiersen, R. (2023). How to Measure Anything in Cybersecurity Risk (2nd ed.). Wiley.

[28] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476.

[29] Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. Computer, 54(2), 80–85.

[30] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. Geneva Papers on Risk and Insurance: Issues and Practice, 47, 698–736.

[31] Bhatt, P., Anand, A., & Yadavalli, V. S. S. (2021). Exploitability prediction of software vulnerabilities. Quality and Reliability Engineering International, 37(2), 648–663.

[32] Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60.

[33] Akbarzadeh, M., Shafieezadeh, A., Choi, J., & Lee, J. (2021). Identifying and analyzing dependencies in and among interconnected critical infrastructures. Sensors, 21(5), 1685.

[34] Zadeh, A. H., Dehghantanha, A., Parizi, R. M., Choo, K.-K. R., & Srivastava, G. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. Decision Analytics Journal, 9, 100328.

[35] Xu, X., Li, Y., Wang, Y., & Zhang, M. (2024). Supply chain cybersecurity investments with interdependent risks under different information exchange modes. International Journal of Production Research, 62(6), 2034–2059.

[36] Gori, T., Bernieri, G., Ferrigno, L., & Laracca, M. (2024). A systematic analysis of security metrics for industrial cyber–physical systems. Electronics, 13(7), 1208.

[37] Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. Applied Sciences, 14(24), 11807.

[38] Bace, M., Dubois, D. J., & Tatar, U. (2024). Resilience against catastrophic cyber incidents: A multistakeholder analysis of cyber insurance. Electronics, 13(14), 2768.

[39] Barrère, M., Hankin, C., Nicolaou, C., El-Amine, K., & Kabbabe, A. (2020). Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. Journal of Information Security and Applications, 52, 102471.

[40] Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM Computing Surveys, 56(8), Article 196, 1–48.

[41] Bellini, E., D'Aniello, G., Flammini, F., & Gaeta, R. (2025). Situation awareness for cyber resilience: A review. International Journal of Critical Infrastructure Protection, 49, 100755.