ARL-TR-9716 • JULY 2023

DEVCOM ARMY RESEARCH LABORATORY

Toward a Scientific Definition of Cyber Resilience

by Sidney C Smith

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TR-9716 ● JULY 2023

Toward a Scientific Definition of Cyber Resilience

by Sidney C Smith
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
July 2023	Technical Report	April 2021–March 2023

4. TITLE AND SUBTITLE
Toward a Scientific Definition of Cyber Resilience

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Sidney C Smith

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DEVCOM Army Research Laboratory
ATTN: FCDD-RLA-ND
Aberdeen Proving Ground, MD 21005-5066

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-9716

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon,
Washington, DC 20301-3030

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD(R&E)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
primary author's email: <sidney.c.smith24.civ@army.mil>.

14. ABSTRACT
This project began with an effort to quantitatively measure cyber resilience because no scientific field of endeavor can truly progress until it can be quantitatively measured. However, before cyber resilience can be measured, it must first be scientifically defined. In an effort to determine if a consensus exists among researchers regarding the scientific definitions of "resilience" and "cyber resilience," we found that no such consensus exists. In fact, experts from several disciplines agree that the word resilience is quickly becoming a meaningless buzz word. This report reviews the literature to establish the current state of the scientific definition of the word resilience. It briefly surveys the literature to discover the qualities of and guidelines for valid scientific definitions. The historic scientific use of resilience is analyzed to discover the path taken to get from its original meaning to the diverse and conflicting meanings that it has today. These concepts are decomposed in a genus differentia analysis untangling the various connotations and separating the related but different concepts. Based upon this analysis, a proposal is made that resilience is part of a family of properties under the umbrella of tenacity.

15. SUBJECT TERMS
Network, Cyber and Computational Sciences, cyber resilience, scientific definition, genus differentia, perseverance, resistance, persistence, tenacity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sidney C Smith
Unclassified	Unclassified	Unclassified	UU	53	19b. TELEPHONE NUMBER (Include area code) 410-278-6235

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures v

Acknowledgments vi

1. Introduction 1

1.1 Challenge 1

1.2 Frustration 2

1.3 Contribution 3

1.4 Organization 4

2. Background 4

2.1 Types of Definitions 4

2.2 Guidelines for Scientific Definitions 5

2.2.1 Wacker's Rules 6

2.2.2 What Scientific Definition is Not 7

2.2.3 Podsakoff et al.'s Recommendations 8

2.2.4 Summary 10

2.3 Measures of Success 10

3. Approach 11

4. Results 12

4.1 Lexical Definitions 12

4.2 Lexical Summary 15

4.3 Historical Review 15

4.3.1 1858: Resilience in Material Science 15

4.3.2 1947: Resilience in Fibers and Fabrics 16

4.3.3 1973: Resilience in Ecology 17

4.3.4 1971: Resilience in Psychology 18

4.3.5 1988: Resilience in the Social Sciences 18

4.3.6 2009: Resilience in the Cyber Domain 20

4.3.7 Summary 24

4.4 Genus Differentia 24
4.5 Contribution of the Word "Cyber" 27
4.6 Operational Definition 29
4.7 Definition Proposal 30
4.8 Measures of Success 31

5. Conclusion 32

6. References 33

List of Symbols, Abbreviations, and Acronyms 44

Distribution List 45

List of Figures

Fig. 1 The stress–strain graph 16
Fig. 2 Decomposition of the quality concept 25
Fig. 3 Decomposition of the dependability concept 25
Fig. 4 Decomposition of the quality concept 27

Acknowledgments

The authors would like to thank the Office of the Under Secretary of Defense Research and Engineering for funding the Quantitative Measurement of Cyber Resilience project, and Dr Alexander Kott for his preliminary work and continuing advice and direction.

1. Introduction

Many are engaged in various efforts to improve cyber resilience, and to improve cyber resilience, it must be measured.[1] Locke[2] commented, "A valid definition of a concept is a prerequisite to valid measurement." This makes the formulation of a valid definition of cyber resilience necessary before cyber resilience may be quantitatively measured. Working backward, a quantitative measure of cyber resilience is required for cyber resilience to be reliably improved. Several authors[2–4] have observed that progress in many areas of research is being hindered by a lack of definitions. Locke[2] observed that some researchers fail to define the concept that they are studying and that others search the literature for a consensus on a definition without ever evaluating that definition. Hibberd[5] observed that some concepts suffer from having too many conflicting definitions and cited three papers[6–8] to substantiate her claim. Brtis[9] observed, “One expert claims that well over 100 unique definitions of resilience have appeared." Cao[10] concurs with this observation saying, “[There] were as many as hundreds of expressions about resilience’s definition.” Aburn et al.[11] found that "there is no universal definition of resilience.” The concept of resilience appears to fall into the category of concepts suffering from too many conflicting definitions.

1.1 Challenge

Locke[2] asserted that good definitions are the epistemological foundation of scientific progress, and sloppy definitions are a major factor retarding intellectual progress. Hibbard[5] observed that without rigorous definitions, “no discipline advances from vagueness and ambiguities of a less than technical language and the follies that result.” Björck et al.[12] observed, “In order for cyber resilience to gain momentum also as an academic research subject, it is important to define the term.” Hoffman and Hancock[13] observed that there has been considerable interest in resilience and “concepts that come to the forefront of concern in this manner are often diluted, simply to become the next ‘flavor of the month’ through both overselling and uncritical use.” They went on to observe, “In such evolutions or revolutions, the definition of terms often proves to be a problematic issue that frequently threatens to derail important conceptual progress."[13] Hosseini et al.[14] conducted a review of definitions and measures of resilience and concluded, “The review of resilience definitions indicates that there is no unique insight about how to define the resilience.” If we are children playing on the seashore finding smoother pebbles or prettier shells,

as Sir Isaac Newton is reported to have observed about himself,[15] then it important that we clearly identify the objects of our research so that others may later synthesis our findings into a larger whole. Absent this clarity, we run the risk of being like the blind men examining the elephant.[16] This is exactly Gigerenzer's[17] point when he spoke about the vague definitions present in integrating theories. He stated, "The practice of using the same label for logically and operationally different phenomena impedes progress."[17]

1.2 Frustration

A literature review searching for a consensus of the definition of resilience, in general, and cyber resilience, specifically, uncovered that the only consensus on the definition of resilience is that there is no consensus on the definition of resilience. Klein et al.[18] conducted a literature review of the definition of resilience in 2003. They observed that from 1973 until 2003, resilience has transformed from a "straightforward concept used only in mechanics" to a "complex multinterpretable concept with contested definitions and relevance."[18] Dillon[19] observed, "There seems to be almost as many different definitions of 'resilience' as there are authors."

In 2008, Norris et al.[20] conducted a literature review of the definition of resilience. They observed that the definitions in use in the social and psychological sciences had diverged so far from the original definition that they wondered if perhaps they should have created their own term. Reid and Botterill[21] conducted an overview of the multiple meanings of resilience in the literature. The key conclusion from their research is that "the term is highly ambiguous, it is used for different purposes in different contexts and in some cases the understandings of the term are diametrically opposed." Woods[22] discussed four concepts of resilience that he found in the literature: (1) resilience as rebound, (2) resilience as robustness, (3) resilience as graceful extensibility, and (4) resilience as sustained adaptability. Cao[10] surveyed the literature surrounding the resilience of transportation systems and divided resilience into maintaining and recovering a required service level after a disruption. Aburn et al.[11] conducted an integrative review of the empirical literature in the health care domain searching for the meaning of resilience. They concluded that there is no universal definition of resilience. They did, however, identify common themes, "Rising above, adaption and adjustment, dynamic process, 'ordinary magic' and mental illness as a marker of resilience."[11] Arghandeh et al.[23] searched the literature for a definition of cyber-physical resilience in power systems and concluded, "There is

no clear and universally accepted definition of cyber-physical resilience for power systems." Hossein et al.[14] conducted a review of resilience in systems engineering. They discovered that "many overlap with a number of already existing concepts such as robustness, fault-tolerance, flexibility, survivability, and agility, among others."[14] Xue et al.[24] explored the science of resilience with a critical review and bibliometric analysis. They summarized the definition of resilience in social and ecological, engineering and disaster, and economic and organizational behavior domains. They concluded, "The definition of resilience is still an important research area."[24]

In 2019, Cottam et al.[25] completed a structured literature review of the definition of resilience in engineered systems. After focusing only on resilience in engineering systems and excluding definitions from psychology, ecology, and socio-ecological systems, they considered 54 papers. They were unable to find any standard defintion of resilience. Futher, many of the definitions that they did find contained the means of achieving resilience as part of the defintion.

Seeing the large number of researchers who have thoroughly reviewed the definition of resilience in the literature and concluded that over the years the definition has expanded to the point of meaningless jargon,[24] another attempt at such a review will not be undertaken in this paper.

1.3 Contribution

Having noted the frustration in the literature about the definition of resilience in general and cyber resilience specifically, the contribution of this report is to review the literature for what constitutes a valid scientific definition. The history of the definition of resilience is then examined. This knowledge is then applied in a genus differentia analysis to propose a valid scientific definition of cyber resilience that will lend itself to a quantitative measurement. Although many have systematically reviewed the literature for the definition of resilience, I know of no other effort to apply the rules for definitions or conduct a genus differentia analysis of resilience.

1.4 Organization

Section 2 reviews the various types of definitions, and the guidelines for good scientific definitions. It then summarizes these into measures of success for evaluating valid scientific definitions. Section 3 outlines the approach to finding a good scientific definition of cyber resilience. Section 4 presents the results. Section 5 provides a conclusion and discussion of future work.

2. Background

Given the state of confusion surrounding the definition of cyber resilience, it is prudent to consider what exactly is a valid scientific definition and how one assesses the validity of that definition. The first area to explore is what are the types of definitions and which type of definition is best suited for a scientific definition. Once a type of definition is chosen, the guidelines for scientific definitions are explored. These guidelines are then consolidated into measures of success.

2.1 Types of Definitions

In his book *Definition*, Robinson enumerated 18 different species of definition.[26] He divided definition into real definitions and nominal definitions. Discovering real definitions was one of the goals of Plato and Aristotle. Socrates was not looking for the meaning of the word when he asked, "What is piety?" He was searching for the meaning of the concept that word represented. A nominal definition is about discovering or assigning a meaning to a word or a symbol.[26] These categories are then further subdivided by their means and purpose. Not every species of definition is covered—only the species that will be encountered later in the search for what makes a valid scientific definition are presented here:

lexical: A nominal definition where the purpose is historical or legislative. The historical purpose states that at some time some people used this word to mean this thing. The legislative purpose states that this word shall be used to mean this thing. These are the kinds of definitions found in dictionaries.[26]

stipulative: A nominal definition declaring that for the following equation or this work, this word or symbol shall mean this thing. These definitions are very common in mathematics.[26]

operational: A real definition that seeks to define a concept by the set of operations used to measure it.[27]

ostensive: A nominal definition which presents an example of the thing that is associated with a word (e.g., defining the word bird by pointing to a bird or showing a picture of a bird).[26]

2.2 Guidelines for Scientific Definitions

Locke[2] observed, "A valid definition of a word (i.e., concept) accomplishes two things: (a) it ties the concept to reality, and (b) it distinguishes the concept from other concepts." Robinson[26] talked about real definitions as analysis, synthesis, and improvement of concepts. When he used the word analysis, he meant breaking a thing down into its component parts.[26] When he used the word synthesis, he meant discovering that the thing in question is part of a larger whole.[26] Real definitions are used to refine or improve concepts by substituting a similar concept that is superior.[26] Hibberd[5] asserted that scientific definitions identify a thing's essential features or conditions. Miller[28] stated, "For scientific research a definition must be flexible enough on fundamental issues to fit many situations and precise enough to permit comparisons." Miller[28] went on to observe that failure to standardize on basic concepts leads to "apples versus oranges" comparisons, which are useless in scientific research.

Cottam et al.[25] observed that definitions should not contain the means of obtaining the object. They relate this to the "what not how" principle.[29] This illustrates the principle expressed by Gen. Patton,[30] "Never tell people how to do things. Tell them what to do, and they will surprise you with their ingenuity." The same principle was the driving force moving the US Department of Defense acquisitions and contracting away from statements of work and toward performance work statements. The danger in including the means to obtain a concept in the definition of the concept is that it leads to measurements that are compliance-based and not independent. Béné[31] discussed this phenomenon in a section he titled, "The circular argument and the need for independent metric." Seville[32] observed that "we need to very careful not to define resilience by the management systems and processes in place to try to build resilience."

Robinson[26] also described what he called a persuasive definition. This kind of def-

inition alters the meaning of a term without changing the emotions associated with the term. He used Plato's definition of "justice" as an example.[26] Since resilience is likely the sexiest new buzz word,[33] it is ripe for this kind of redefinition. All agree that resilience is a "good" thing. There is a temptation to leverage this to expand the definition to include appealing concepts and remove from the definition less-than-appealing concepts. We can see an example of this in the work of Phillips and Chao.[34] They stated, "Resilience is not simple survival, bounce-back, or homeostasis."[34] They clearly prefer the concept of positive evolution through stress over the concept of homeostasis; however, the problem with this statement is that the lexical definition states that bounce back is exactly what the world resilience means and has meant for centuries—millennia if the Latin root is considered. Olsson et al.[35] explained why the concept of resilience as positive growth after stress gains traction in their field and why resilience as rebound to a previous state is unappealing.

Several researchers have collected rules, cautions, and recommendations for valid scientific definitions. John Wacker, in his theory of formal conceptual definitions, presented eight rules for formal conceptual definitions.[4] In her article "What is Scientific Definition?" Fiona Hibberd[5] presented a list of seven things that a scientific definition is not. Podsakoff et al.[3] summarized their article "Recommendations for Creating Better Concept Definitions in the Organizational, Behavioral, and Social Sciences" with 10 recommendations. Excerpted definitions are presented in Sections 2.2.1–2.2.3.

2.2.1 Wacker's Rules[4]

Rule 1: Definitions should be formally defined using primitive and derived terms. Formal conceptual definitions should differentiate between formal concepts and non-formal measurable terms. All definitions should follow the "rule of replacement."

Rule 2: Each concept should be uniquely defined. It should exclude (as many as possible) shared terms with other definitions to reduce confusion with related concepts. This rule means that the formal conceptual definitions denotation matches as closely as possible match its connotation.

Rule 3: Definitions should include only unambiguous and clear terms. Put another way, do not use vague or ambiguous terms.

Rule 4: Definitions should have as few as possible terms in the conceptual definition to avoid violating the parsimony virtue of "good" theory.

Rule 5: Definitions should be consistent within the production/operations management field. That is, formal conceptual definitions should be the similar as possible between studies.

Rule 6: Definitions should not make any term broader. New definitions should not expand the concept to make it broader and less exclusive.

Rule 7: New hypotheses cannot be introduced in the definitions. In production/operations management, the definitions should not include instances where only 'good' events happen.

Rule 8: Statistical tests for content validity must be performed after the terms are formally defined. These empirical tests are not tests of the conceptual validity of a concept but rather are used to test if the formally defined concepts sample the conceptual domain.

2.2.2 What Scientific Definition is Not[5]

(i) It is not conventional – criteria for the term's use have not been decided by agreement and so established by convention *without referencing the kind's essential features.*

(ii) It is not stipulative – no-one is arbitrarily assigning a meaning to the expression "dissociative identity" or the "reiteration effect," for example.

(iii) It is not nominal – we are not assuming that the kinds exist in name only and that what we are defining is nothing more than the name/word or the idea/imagined features attached to the name/word (e.g., the word "unicorn") or defining a word by using other words. Our concern is scientific, not linguistic, because our working hypothesis is that there are psychological relations, processes, or states with the features or conditions indicated.

(iv) It does not confuse *is* with *does* – we are not conflating what something is with a description or definition of its goal, purpose, or function. Conventional definitions are inclined to define something by its function or causal role, e.g., a heart is a pump, an eye sees, a shoe protects the foot, but this is not to identify the essential features of the heart, eye, or shoe. "What is X?" is a question different from "what does X do?" or "what function/role does X have?" or "what are the effects of X?" There is nothing wrong with a functional definition as long as what the kind *does* is not muddled with what the kind *is*.

(v) It is not operational – we are not defining or giving meaning to a kind "...by spelling out what the investigator must do to measure it and evaluate that measurement." Nor is it "... a sort of manual of instructions to the investigator" (Kerlinger,[36] and Lee, 2000, p. 42).

(vi) It is not ostensive – we are not pointing to an example of hindsight bias and saying "hindsight bias is this" or "the term 'hindsight bias' means this." To refer to an example of X is not to describe the kind X's essential features. (vii) It is not classification – we are not collecting examples of an empirical phenomenon and making the case that each example is a member of some particular class. We classify according to our knowledge, needs, and interests. In the scientific context, an outcome will be a collection of things (a class) classified according to the kind of thing they are, that is according to the kind's essential features. So, classification depends on definition and, therefore, cannot be definition. For instance, we could point to a particular act of tweeting a threatening message through social media and make the case that this act exemplifies aggression and, therefore, belongs to the class of aggressive behaviours. But "making the case" is not definition for it depends on the definition of aggression, on what kind of behaviour aggression is. It depends on the conditions required for membership to that class, those conditions being the essential features that run through every act of aggression necessarily. This definition-classification distinction may not always be well understood. For instance, the claim that DSM-5 allows more individuals to be diagnosed with a mental disorder than previous editions does not amount to an "expansion of the concept of mental disorder" (the title of Boysen and Ebersole, 2014),[37] because the definition of mental disorder hasn't altered. It is rather that the number of cases of mental disorder (the cases in this class) is likely to increase because the diagnostic criteria have been made more inclusive.

2.2.3 Podsakoff et al.'s Recommendations[3]

1. Are the techniques used to collect a representative set of definitions (*e.g.*, survey the literature, interview subject matter experts, compare the construct with its opposite pole, etc.) described in the paper? (If so, is it clear how the researchers used the techniques to develop the concept's definition?)
2. Does the definition describe the type of property the concept represents? (Does the definition specify the nature of the phenomenon (*e.g.*, intrinsic characteristics, thoughts, feelings, perceptions, actions, or performance metrics) to which the focal concept refers?)
3. Does the definition describe the entity to which the property applies? (Does the definition specify the object or event [*e.g.*, person, task, pro-

cess, relationship, dyad, group, team, organization, culture, etc.] to which the property applies?)

4. Does the definition describe the theme of the concept and identify its necessary and jointly sufficient or central attributes (depending upon the concept structure)? (For a concept having a necessary and sufficient concept structure, does the definition specify: [a] the concept's essential attributes/characteristics and [b] the concept's unique attributes/characteristics? For a concept having a family resemblance concept structure, does the definition: [a] specify the set attributes that are shared by subsets of cases of the concept, [b] identify the central attribute[s] shared by the most cases of the concept, and [c] identify the most prototypical cases [*i.e.*, those that possess the greatest number of shared attributes?])
5. Is the concept defined solely in terms of examples? (Although it is helpful to provide concrete examples of the focal concept through the process of instantiation, the examples should not serve as the primary mechanisms for defining the concept.)
6. Does the definition specify the dimensionality of the concept? (If so, are the properties, entities, and conceptual themes of the subdimensions adequately described, and is it clear whether the subdimensions are conceptualized as manifestations or defining characteristics of the higher-order concept?)
7. Does the definition specify the stability of the concept? (That is, does the definition specify whether the concept is considered to be fairly stable or fairly dynamic over time and across situations?)
8. Does the definition explain how the focal concept differs from related concepts? (Does the definition identify which attributes of the focal concept are not possessed by [or shared with] related concepts and include a discussion of this in the paper?)
9. Is the concept defined solely by reference to its consequences or antecedents? (Although it is important to specify parts of the nomological network of the concept in order to help clarify the theoretical relationship between the focal concept and other concepts, the conceptual definition should not be based exclusively on a description of the antecedents and consequences of a concept.)
10. Does the definition of the concept use ambiguous, vague, or ill-defined terms? (Is the concept's definition clear and concise and relatively de-

void of technical jargon? Can a layperson, not expert in the domain, understand the definition?)

2.2.4 Summary

Considering the rules, cautions, and recommendations presented above, the most succinct definition of a scientific definition is given by Locke[2] in that it ties a word to a concept and that concept to reality, distinguishing it from other concepts.

2.3 Measures of Success

Since many of the guidelines discussed previously overlap, it is useful to consolidate them to provide some measures of success that may be used to evaluate the validity of definition discovered through this research. The following list consolidates these guidelines into five measures of success.

1. *A valid scientific definition is a real definition associating a word to a unique concept that may be observed and measured.* The statement satisfies Locke's[2] requirement that a valid definition ties a concept to reality. It embodies Wacker's[4] second rule that concepts should be uniquely defined and the eighth rule about tests for validity. It addresses Hibberd's[5] concerns that scientific definitions are not nominal or ostensive. Although there is a requirement for observability and measurement, the definition is not objective in that it is solely composed of the procedures for measuring it. This also precludes ostensive definitions and those based merely upon classification.[3,5]

2. *A valid scientific definition is clear.* This statement embodies Wacker's first, and third rules,[4] and Podsakoff et al.'s 10th recommendation.[3]

3. *A valid scientific definition differentiates the concept from related concepts.* This statement satisfies Locke's requirement that a valid definition distinguishes the concept.[2] It addresses Wacker's second rule and Podsakoff et al.'s fourth and eighth recommendations.[3,4]

4. *A valid scientific definition is consistent with the historical use of the word.* Although philosophers and scientists have struggled to find words to described the objects of their considerations and sometimes stretched a word to describe a previously unnamed concept, this new meaning should be consistent with the word's original meaning and should not be used in place

of a word with a traditional meaning closer to the concept. This addresses Wacker's fifth rule about consistency and sixth rule about broadening terms.[4] This also combats the tendency to expand the definition of a term for persuasive purposes.[26]

5. *A valid scientific definition should not contain the means for attaining it.* This addresses Cottam et al.'s concerns[25] as well as Patton's observation.[30] There certainly is a place for suggesting methods for obtaining a goal; however, including these in the definition tends to focus the measurement of the concept more on compliance to the suggestions and less on the accomplishment of the goal.

3. Approach

The approach to discovering a valid scientific definition of cyber resilience begins with a review of the lexical definition of resilience. It proceeds to a literature review with a focus on the history of the scientific use of the word resilience. Then a genus differentia analysis is presented. The contribution of the qualifier cyber is discussed, and an operational definition of cyber resilience is considered. The definition of cyber resilience resulting from this analysis is proposed. Finally, this definition is compared to the measures of success outlined in Section 2.3.

As Locke[2] recommended, the search for a scientific definition of resilience begins by consulting several dictionaries. Although a scientific definition is not a nominal definition[5] and lexical definitions are nominal definitions,[26] the purpose of the word is still to communicate. The scientific definition may be more precise than the lexical definition; however, it should still be within the bounds of the lexical definitions to avoid confusion. If the scientific definition of resilience is outside the scope of the lexical definition of resilience, then resilience is probably the wrong word.

Although Locke[2] criticized academics who only search academic literature for the definition of a concept, a literature a review is presented here to discover the various ways that resilience has been defined both inside and outside the cyber domain. This review is organized to trace the history of the meaning of resilience in an effort to track its evolution and understand the expansion that has led to the current state of meaninglessness.

The standard account of the scientific definition has used the genus differentia model that has been employed since Plato. Although there is no longer a requirement that scientific definitions be stated in this form, this form of definition satisfies Locke's requirement that a definition tie a concept to reality and distinguish it from other concepts.[2] This exercise allows the examination of the words in common use surrounding the concept of resilience and allows the establishment of its place in that context.

This quest is for a scientific defintion of cyber resilience; however, to this point the focus has been upon the term resilience because that is the term that carries the most confusion. It is important to consider what the addition of the term cyber adds to and excludes from the definition.

Although a scientific definition is more than an operational definition, it is appropriate to give some thought as to how to measure this concept. The ability to measure something also clearly ties it to reality, which is one of Locke's requirements. Furthermore, it was the desire for a quantitative measurement of cyber resiliences that was the catalyst for this search for a scientific definition.

4. Results

In this section the search for a scientific definition of resilience begins by examining the definitions for resilience as found in dictionaries. Next, the scientific definitions of resilience are traced through history. An analysis of the genus and differentia of the concept of cyber resilience is presented. Finally, this definition is assessed against the measures of success outlined in Section 2.3.

4.1 Lexical Definitions

The root of the words resilient and resilience is the word resile. The word resile comes to English from the the French *resiler* and the Latin *resilire*. It is composed of *re* meaning back and *salire* meaning jump.[38–41] The word carries the meaning of jumping back, recoiling, springing back, or resuming an original position.[38–41] The following are definitions for the word resilience taken from several different dictionaries spanning several decades from oldest to youngest.

1955: ***Webster's New World Dictionary of the American Language***[42]

1. The quality of being resilient; ability to bounce or spring back into shape, position, etc. after being pressed or stretched; elasticity.
2. The ability to recover strength, spirits, good humor, etc. quickly; buoyancy.

1980: ***The Random House College Dictionary***[43]

1. The power or ability to return to the original form or position after being bent, compressed, or stretched; elasticity.
2. Ability to recover readily from illness, depression, adversity, or the like; buoyancy.

1983: ***Webster's New Twentieth Century Dictionary of the English Language Unabridged***[44]

1. The act of leaping or sprining back; a rebounding; as, the resilience of a deformed body after the removal of the deforming force.
2. The quality of being resilient; ability to bounce or spring back into shape, position, etc. after being pressed or stretched; elasticity.
3. The ability to recover strength, spirits, good humor, etc. quickly; buoyancy.
4. In mechanics, the work done by a body in springing back.

1993: ***The New Shorter Oxford English Dictionary on Historical Principles***[45]

1. a. The action or an act of rebounding or springing back. b. Recoil from something; revolt.
2. Elasticity; spec. the amount of energy per unit of volume that a material absorbs when subjected to strain, or the maximum value of this when the elastic limit is not exceeded.

3. The ability to recover readily from, or resist being affected by, a setback, illness, etc.

2006: ***The American Heritage Dictionary of the English Language***[46]

1. The ability to recover quickly from illness, change, or misfortune; buoyancy.
2. The property of a material that enables it to resume its original shape or position after being bent, stretched, or compressed; elasticity.

2019: ***The Merriam-Webster Dictionary***[47]

1. The ability of a body to regain its original size and shape after being compressed, bent, or stretched.
2. An ability to recover from or adjust easily to change or misfortune.

2022: ***Cambridge Dictionary English Dictionary***[48]

1. The ability to be happy, successful, etc. again after something difficult or bad has happened.
2. The ability of a substance to return to its usual shape after being bent, stretched, or pressed.

2022: ***2022: Macmillan Dictionary***[49]

1. Someone's ability to become healthy, happy, or strong again after an illness, disappointment, or other problem.
2. The ability of a substance or object to return to its original shape after being bent, stretched, or pressed.

4.2 Lexical Summary

All of these definitions describe the concept of recovering or returning to the original shape or condition after some external force has caused a change. The terms spring, bounce, rebound, and buoyancy are used to describe this sense of the word, which is consistent with the meaning of resile. The two exceptions are the third definition from the Oxford dictionary, which includes the concept of resisting,[45] and the second definition from the Merriam-Webster's dictionary, which includes the concept of adjusting.[47]

4.3 Historical Review

4.3.1 1858: Resilience in Material Science

In 1858, Rankine used the word to describe the effects of stress and strain on solids.[50] In his discussion, he defined stress as the force applied to an object, and strain as the alteration observed in the object.[50] Stiffness is the resistance to elastic deformation. Elasticity is when the object recovers its original shape when the stress is withdrawn. Plasticity is when the object does not retain its original shape when the stress is withdrawn.[50] Fracture is the point at which the object is divided into parts. Toughness is the greatest strain that the body will bear without fracture.[50] Resilience is the quantity of mechanical work required to produce the proof strain.[50]

Resilience has retained this meaning in material sciences to this day. Ahmmad et al.[51] used this same definition of resilience in their paper "Ductility performance of lightweight concrete element containing massive palm shell clinker." This concept is expressed in a stress–strain graph from that paper Fig. 1.

There is room for some blurring of these concepts because resilience cannot be measured without first measuring stiffness, and toughness cannot be measured without first measuring resilience. However, Ahmmad et al.[51] pointed out there can be advantage of ductility or resilience and toughness over stiffness. Standard concrete could be very strong, but since that strength was primarily in stiffness, when it failed, it failed catastrophically. The concrete that they made with palm shell clinkers as the aggregate had higher ductility (i.e., resilience and toughness) failing more safely being permanently deformed but not breaking.

In this context, the properties of stiffness, resilience, and toughness have neither a negative nor a positive connotation. Sometimes a material with a high resistance is

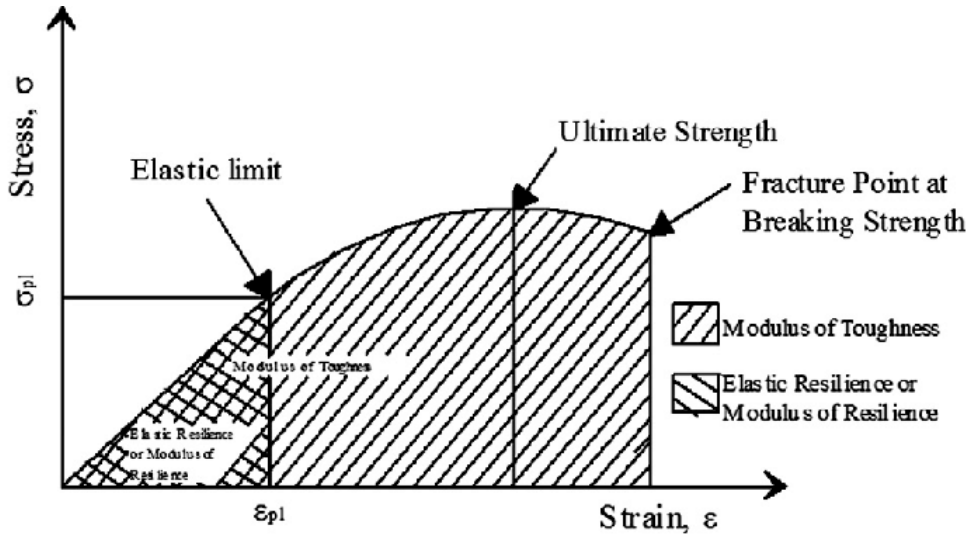

Fig. 1 The stress–strain graph[51]

required; a resilient ball bearing would not be useful. Sometimes a material with a high resilience but lower resistance is required; a spring without resilience would not work. Sometimes a material with a high toughness but low resilience is required; a rivet would be useless if it always returned to its original shape. There are even times when brittle materials are required; a sheer pin that bent and did not break would not function properly.

4.3.2 1947: Resilience in Fibers and Fabrics

In 1947 when Dillon[19] wrote his article "Resilience of Fibers and Fabrics," the definition of resilience in this context had grown and diversified until there were as many definitions as there were authors. Dillon was talking about the mathematical definition and methods used to measure resilience. The materials that Rankine[50] studied obeyed Hooke's law; however, some fibers and fabrics do not. Hooke's law states that within the elastic range the stress and strain scale linearly.[52] Some fibers and fabrics which are resilient in that they regain their shape after stress do not do so quickly. These facts make the measure of resilience as a function of work problematic. The basic distinction between stiffness, resilience, and toughness remained; however, new methods for measuring this were necessary. Dillon finished his work saying, "The obvious conclusion from this study is that resilience is a much abused and poorly defined term and that much remains to be learned about its significance and the factors controlling it, in single fibers, bulked fibers, and fabrics."[19]

Hoffman[53] defined resiliency as "the capability of a substance to return to its original state at some later time after the removal of the deforming stress." He added time to stress and strain as a component of resilience. The materials that Rankine considered immediately returned to their original state once the stress was removed. Wool more gradually returns to its original state. His proposed definition is "a stress–strain-time property of a material, characterizing the completeness of recovery from deformation and varying in kind with the modulus of elasticity and rate of recovery."[53]

Resilience gains a positive connotation because fabrics with too much stiffness are uncomfortable to wear, and fabrics without resilience stretch, becoming baggy in the joints. The word resilience begins to mean fit for a particular purpose (e.g., "An experimental tire made of woolen cords overheated badly; therefore, wool is not resilient."[53])

4.3.3 1973: Resilience in Ecology

In 1973, Holling[54] applied the term resilience to ecological systems. He stated, "Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist." Holling faced problems beyond the scope of previous research into resilience. How does one measure the ability of a system to return to a previous state when the state of the system is constantly changing? Ecologies may be said to exist in a stable equilibrium. Resilience measures the amount of stress that the system can absorb before a different stable equilibrium is established. Gruemm[55] proposed a measurement of resilience based upon stability theory using differential topology where the state space of the system is divided into basins with each basin containing an attractor. A system is considered resilient against a certain stress if the system returns to the same basin.[55] Bodin and Wiman[56] also pointed to the link between resilience and stability in ecology.

The distinction between stiffness and resilience starts to blur. This treatment distinguishes fracture or extinction, plastic change when the system moves to a different basin, and elastic change when the system returns in the original basin. It does not distinguish zero change, or stiffness, from elastic change in that both would result in the system being in the original basin. Gruemm's work seems to demonstrate that what Holling was actually describing was stability and not resilience. Xue et al.[24]

pointed to Holling's work as the beginning of an explosion in resilience research stating, "The definition of resilience in different categories are all derived from the ecology domain." This may be one of the reasons for proliferation of the confusion between stability and resilience.

4.3.4 1971: Resilience in Psychology

The study of resilience in psychology began in orthopsychiatry. While studying individuals with high-risk factors for developing psychosis, it was discovered that some of the subjects thrived despite very high-risk factors. These individuals were originally called invulnerable, but this was later replaced with the term resilient.[57–60] Luthar et al.,[61] leveraging this previous work, said, "Resilience refers to a dynamic process encompassing positive-adaption within the context of significant adversity. Implicit within this notion are two critical conditions: (1) exposure to significant threat or severe adversity; and (2) the achievement of positive adaptation despite major assaults on the developmental process." Connor and Davidson.[62] viewed resilience as a measure of stress coping ability. Wald et al.[63] stated, "Fundamentally, resilience refers to positive adaptation, or the ability to maintain or regain mental health, despite experiencing adversity."

Research in psychology discovered a phenomenon in the interaction between stress strain that does not exist in solids, fibers and fabrics, and was as yet undiscovered in ecological systems. This phenomenon is that some subjects become stronger after being exposed to stress. The phenomenon itself is not new. Fleming and Ledogar[64] observed, "The concept of positive adaptation despite adversity has existed practically since humans began reflecting on their own behaviour." The benefits of exercise, which involves subjecting the body to stress for growth, had been well known for a very long time. In *The Epistle of Paul to the Romans* (5:3–5), he spoke of the ability for tribulation to lead to growth in the first century.

However, this was the first time that growth through stress is associated with the word resilience. There is also a further blurring of the line between resisting and rebounding. The positive connotation of the word resilience grows significantly. Resilience is now seen as a very desirable quality.

4.3.5 1988: Resilience in the Social Sciences

When we talk about resilience in social sciences, we include the study of resilience in environmental, economic, and political systems. Wildavsky,[65] while considering

the resilience of social systems, defined resilience as "the capacity to cope with unanticipated danagers after they have become manifest, learning to bounce back." He also observed that stress may be necessary for the development of resilience.[65] Comfort[66] defined resilience as "the capacity to adapt existing resources and skills to new situations and operating conditions." Adger[67] and Berkes et al.[68] merged the concepts of social and ecological resilience creating the concept of social-ecological systems.

Efforts were undertaken to measure and improve the resilience of communities to disasters.[69,70] Bruneau et al.[69] defined resilience as "the ability of social units (e.g., organizations, communities) to mitigate hazards, contain effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes." Norris et al.[20] defined resilience as "a process linking a set of adaptive capacities to a positive trajectory of functioning and adaption after a disturbance." Fleming and Ledogar[64] defined resilience as "positive adaption despite adversity."

In 2011, President Obama issued a Presidential Policy Directive 8[71] that defined resilience as "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies." The National Research Council[72] defined resilience as "the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events." Béné[31] defined resilience as "any capacity and skills, and action, strategy, investment and anticipation, which helps individual, households and communities to anticipate, absorb, accommodate, or recover from the impacts of a particular adverse event (shock, stress, or (un)expected changes)."

Alexander[73] examined the historical use of the word resilience in the context of disaster risk reduction. He also talked about the conflict between those who hold that resilience is transformation rather than preservation.[73] Southwick et al.[74] recorded Dr Rachel Yehuda using an expression made popular by Timex watch commercials defining resilience as "the ability to 'take a licking and keep on ticking.'" Musman and Agbolosu-Amison[75] defined resilience as "the persistence under uncertainty of a system's mission-oriented performance in the face of some set of disturbances that are likely to occur given some specified timeframe." Cao[10] defined resilience as "the ability of system to become healthy and strong again after a disruptive event."

Larkin et al.[76] defined resilience as “the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.” The European Commission[77] defined resilience as “the ability of an individual, a household, a community, a country, or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development.” Natural and man-made disasters also illustrated the need for resilient organizations, and the means of building resilience began to creep into the definition of resilience.

At this point the word resilience becomes an umbrella term that covers every aspect of the stress–strain relationship up to the point of fracture. It is used to cover a system’s ability to resist stress, to rebound from stress, to bend but not break, and to grow through stress. Words like prepare and plan, which are means to becoming resilient, begin to creep into the definition. There is even a marked preference for the connotation of growth over rebound as Phillips and Chao[34] asserted and Olsson et al.[35] explained.

4.3.6 2009: Resilience in the Cyber Domain

In the cyber domain, the word resilience has seen every form of abuse seen in other fields. It has been defined expansively to cover every aspect of the interaction between cyber stress and cyber strain. The definition has been expanded to cover the means of attaining resilience. Unique to the cyber domain, there has been an effort to distance cyber resistance or cybersecurity from cyber resilience.

4.3.6.1 Expanded Definition

The scope of resilience expanded to encompass “the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations."[78] Wood and Branlat,[79] while examining how adaptive systems fail, defined resilience as a form of adaptive capacity. The World Economic Forum[80] defined cyber resilience as “the ability of systems and organizations to withstand cyber events, measured by the combination of mean time of failure and mean time to recovery.”

Informally, resilience can be defined as the ability of an organization to continue to function, even though it is in a degraded manner, in the face of impediments that affect the proper operation of some of its components.[81] Pawlikowski et al.[82] defined resilience as “the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary

actions." Musman and Agbolosu-Amison[75] defined resilience as "the persistence under uncertainty of a system's mission-oriented performance in the face of some set of disturbances that are likely to occur given some specified timeframe." Björck et al.[12] defined resilience as "the ability to continuously deliver the intended outcome despite adverse cyber events." Cureton and Brtis[83] stated, "Resilience is the ability to provide required capability in the face of adversity. The scope of resilience includes the ability to avoid, withstand, and recover from adversity (the objective is required capability, not system stasis)." Khan et al.[84] defined cyber resilience as "the ability of a system to resist against (or minimize) the potential damage in order to maintain system state within an accepted operational level in response to any external threat or attack."

The Committee on National Security Systems (CNNS) Glossary[85] defined operational resilience as "the ability of a system to resist, absorb, and recover from or adapt to an adverse occurrence during operation that many cause harm, destruction, or loss of ability to perform mission-related functions." Cybenko[86] loosely defined cyber resiliency as "an information processing system's ability to return to some level of desired performance after a degradation of that performance." Brtis[9] defined resilience as "the ability to deliver capability in the face of adversity." Baros et al.[87] defined cyber-physical resilience as "the ability to withstand the combined presence of both cyber attacks and physical faults." Special Publication 800-53[88] defined *Information System Resilience* as "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs." Cottam et al.[25] defined a resilient system as "a system that is able to successfully complete its planned mission(s) in the face of disruption(s) (environmental or adversarial), and has capabilities allowing it to successfully complete future missions with evolving threats."

Clark and Zonouz[89] spoke of resilience requiring toughness and elasticity. They further went on to state, "This definition of resilience is analogous to the definition of resilience in materials sciences, namely, the amount of energy that must be exerted to steer the system to a state from which it cannot recover to the stable equilibrium." Bellini and Marrone[90] proposed a "novel holistic definition able to accommodate in a unique coherent vision the existing multiple facets." Faulkner

et al.[91] stated, "*Cyber Resilience:* brings together the capabilities of cybersecurity, business continuity, and enterprise resilience. It applies holistic security strategies to help federal agencies and other organizations respond quickly to threats so they can minimize the damage and continue to operate under attack."[91] Andersson et al.[92] leverage Laprie's[93] definition that resilience is "an extension of dependability when facing changes." Beling et al.[94] said that resilience is "a high-level property relating to the capacity of the systems to recover from unwanted loss of function." The ISACA Glossary[95] defined cyber resilience as "the ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect."

4.3.6.2 Inclusion of the Means

Brtis et al.[96] provided a list of means of obtaining resilience. Among these means may found anticipation, and adaptability. Certainly the ability to anticipate, withstand, and adapt are all very desirable properties. Although they may be employed by resilient systems, they are not themselves resilient, and systems that do not employ them may still be considered resilient. Observe the usage of these terms in the following definitions to see how these means of attaining resilience have crept into the definition.

In 2013, President Obama released Presidential Policy Directive 11[97] that defined cyber resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions." The Committee on Payments and Market Infrastructures[98] defined cyber resilience as "the ability to anticipate, absorb, adapt to and/or recover from disruption cause by cyber attack." Azebbi[99] stated, "Cyber resilience is being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world." DiMase et al.[100] cited the National Academy of Sciences[101] definition of resilience see Section 4.3.5.

Dessavre and Ramirez-Marquez[102] said, "Cyber resilience (or resiliency) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources." Bodeau et al.[103–106] stated "Cyber resilience (or resiliency) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources." Markin and Samans[107] in the *Cyber Resilience Playbook for Public-Private Collab-*

oration defined cyber resiliences as "the capability to detect threats, prevent their infiltration or at least confine their expansion, manage their effects and deny their recurrence; the notion of adaptability is at the core of resilience, as is being able to continue ordinary operations." Carias et al.[108] cited the Spanish National Cybersecurity Institute defining cyber resilience as the "ability of a process, business, organization, or nation to anticipate, withstand, recover, and evolve in order to improve their capabilities in the face of adverse conditions, stress, or attacks to the cyber resources it needs to function." Brtis et al.[96] identified avoiding, withstanding, and recovering from adversity along with evolving and adapting as the means to acheive cyber resilience. Ross et al.[109] defined cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions."

As an example, the definition given by Bodeau et al.[105] not only included every aspect of the stress–strain relationship short of fracture, but it also included many of the means of obtaining resilience in the definition. Further, their *Cyber Resiliency Metrics Catalog* established exactly the compliance-based measure that results from the inclusion of means into the definition.[105]

4.3.6.3 Distinct from Cybersecurity

There is also a realization that perfect resistance to cyber threats, although desirable, is impractical.[84,108,110–113] Specifically, Whelihan et al.[112] defined cyber resilience as "a system property in which a system is designed to withstand the *successful* exploitation of vulnerabilities and continue to meet mission goals." Alexeev et al.[110] equated cyber resilience to the question, "Can systems be designed such that they continue to function while compromised?" Deutscher et al.[111] defined a resilience as the "ability to continue to function after the company suffers a breach (as it inevitably will) and to recover gracefully after even a serious security lapse." Observing that, past a certain point, the cost of enhanced cybersecurity quickly outpaces the benefits, there is a desire to ensure that systems have the ability to continue to operate after a compromise. This ability is often called resilience. It is consistent with this call for resilience that Linkov and Kott[113] observed that it "has been associated with a shift in safety paradigm acknowledging that system coping is important when prevention is impossible."

4.3.7 Summary

There has been an explosion in research focused on resilience in the past few years. Xue et al.[24] tracked the number of papers published with resilience in the title showing rapid nonlinear growth from a few papers in 1986 to over a thousand papers in 2014. With this vast growth in research, it should not be surprising to find a similiar expansion in the meaning of the term resilience. As Klein et al.[18] observed, "Resilience has become an umbrella concept for a range of system attributes that are deemed desirable." Since the early 1970s, the definition of resilience has expanded from elastic deformation to include every aspect of strength (*i.e.*, stiffness, spring, and toughness.) It has grown beyond the original concept of strength to include positive change or growth. In the cyber community, it has taken on the connotation of continuity of operation after a compromise. As the connotation of the word resilience gains in desirability and many are striving to encourage the improvement of resilience, means like adaptability and planning have been added to the definition. Resilience has a become a panchreston.[114] The problem with a panchrestron is that when a word means everything, it means nothing.

4.4 Genus Differentia

The exploration of the genus and differentia of resilience follows the pattern of Aristotle and not Linnaeus. There is no claim that the taxonomy is in anyway exhaustive.

At a high level one can say that resilience is a quality attribute. Miller,[28] leveraging Juran,[115] defined quality as "fitness for use" with the understanding that this has two aspects: "product features that meet customer needs and freedom from defects." Barbacci et al.[116] and the Institute of Electrical and Electronics Engineers (IEEE) Standard 1061[117] defined software quality: "Software quality is the degree to which something possesses a desired combination of attributes (e.g., reliability, interoperability)." However, the concept of quality has expanded to cover almost every aspect of a system. Barbacci et al.[116] decomposed quality into performance, dependability, security, and safety. This is illustrated in Fig. 2 where the italic terms represent the path toward resilience.

Since Laprie[93] defined resilience in terms of dependability, 'Dependability when facing changes." Dependability seems to be appropriate aspect of quality to pursue. Littlewood and Strigini[118] define dependability as the set of systems properties

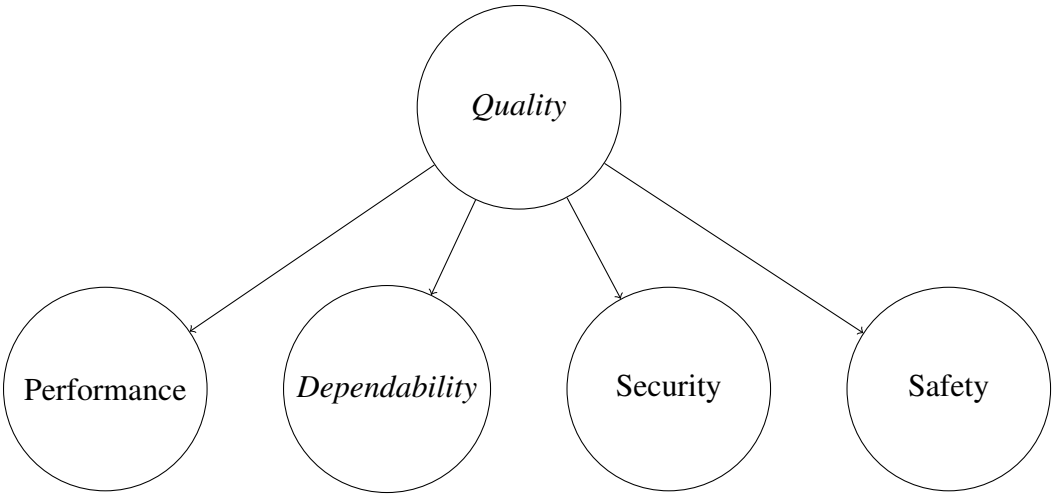

Fig. 2 Decomposition of the quality concept

"that allows us to rely on a system functioning as required." Laprie[93] went on to refine that definition, "Dependability is that property of a computer system such that reliance can justifiably be placed on the service it delivers." Barbacci et al.[116] in the paper, "Quality attirbutes" divide dependability into several attributes, including availability, reliability, safety, confidentiality, integrity, maintainability. This is illustrated in Fig. 3 where the italic terms represent the path toward resilience.

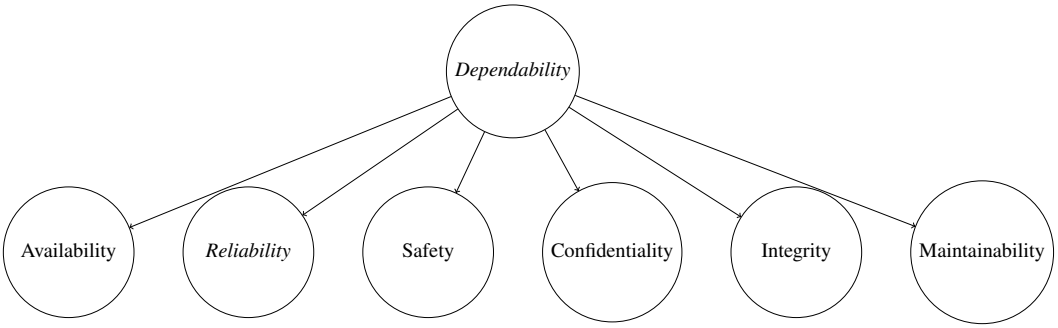

Fig. 3 Decomposition of the dependability concept

It is important to differentiate between dependability and security since both dependability and security are concerned with availability, confidentiality, and integrity. When Bishop[119] defined computer security, he talked about requirements, policies, and mechanisms. Security is about having the mechanisms to implement the policies that fulfill the requirements aligning well with the "fitness for use" aspect of quality. Dependability is about these mechanisms working correctly and

continuing to work correctly during adverse conditions aligning well with the "free from defects" aspect of quality.

Woods[22] described four concepts of resilience: rebound, robustness, graceful extensibility, and sustained adaptability. Robustness is "the ability of a system to function correctly in the presence of disturbances."[120] A robust system is one where small disturbances lead to small deviations and the effect of sporadic disturbances disappear over time.[121] It is clear that a robust system would be more resilient than a fragile system; however, a system could be robust and still ineffective in a hostile environment since the only requirement is that it be able to recover from sporadic disturbances.

The concepts of graceful extensibility and sustained adaptability map directly to the dependability concept of maintainability. These are certainly desirable qualities and could contribute to the resilience of a system if measured over a system's lifetime; however, they would contribute very little if resilience is measured over a mission. Therefore, they would be better considered as a means of implementing resilience than as part of the definition of resilience itself. This leaves the concept of rebound, which maps directly to the lexical definition of resilience.

Barbacci et al.[116] defined reliability as "a measure of the ability of a system to keep operating over time." The ability to keep operating in the face of cyber stress is covered by reliability; however, reliability is a broader term because it applies to continued function in the face of normal wear and tear. There is a need for a term that encompasses the full spectrum of the relationship between stress and strain. Rankine[50] used the word strength; however, that word is so common as to be too vague. Furthermore, it was never applied to positive adaptation through stress as metals do not demonstrate that ability. Many now use the word resilience for this, but that has led to much confusion. Hoffman[53] used the word tenacity, and it seems a fitting word to describe the relationship between to stress and strain to the point of fracture.

Tenacity may be further decomposed into resistance or stiffness, resilience or elasticity, persistence or toughness, and perseverance or positive adaptation. This is illustrated in Fig. 4. Resistance speaks to a system's ability to withstand stress without a perceptible degradation in performance. Resilience speaks to a system's ability to absorb stress elastically; that is, performance will perceptibly degrade but return

when the stress is removed or nullified. Persistence speaks to a system's ability to absorb stress plastically; that is, the system will continue to function at an acceptable level of performance in the face of stress. It also carries the idea of bending but not breaking easily. In addition, there is the additional case of perseverance or adaptability. Perseverance is plastic change; however, this change improves the tenacity of the system. An example would be recovering from an illness where the recovery builds immunity providing enhanced resistance in the future. All of these are important concepts that many of the definitions of resilience in the literature confuse, making it difficult to distinguish between them.

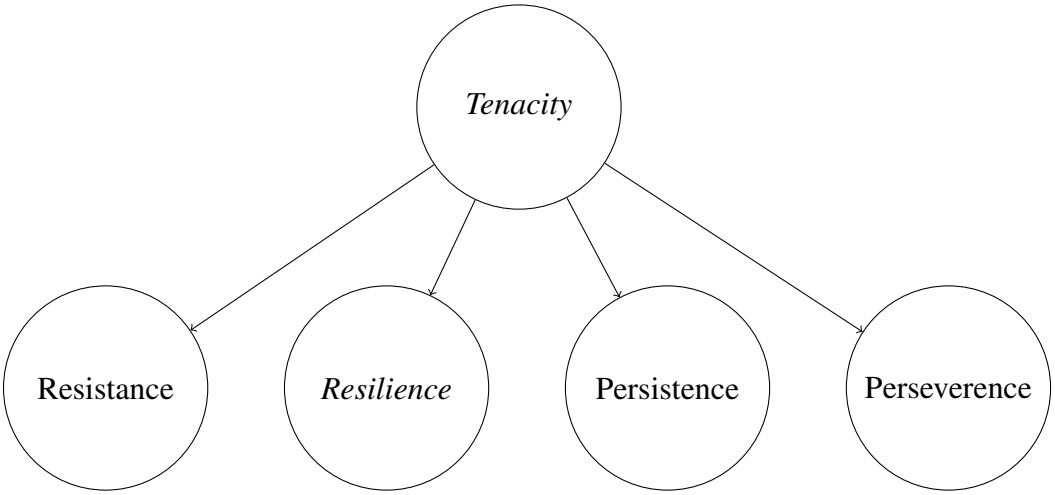

Fig. 4 Decomposition of the quality concept

Resilience then is a property of tenacity. Where tenacity describes the ability of a system to withstand stress without failure. Resilience specifically is the elastic response to stress where the system is measurably impacted but returns to the former state when the stress is removed or nullified.

4.5 Contribution of the Word "Cyber"

"Cyber" means "involving, using, or relating to computers, especially the internet."[122] Using the word cyber to modify resilience produces three similar but different connotations. It could mean that a system is resilient against cyber-stress. It could also mean that a cyber system is resilient against stress. Finally is could mean that a cyber system is resilient against cyber stress.

It is the author's opinion that there is general agreement that the recovery of strain

on a cyber system caused by cyber stress must be considered cyber resilience. At the same time, it is difficult to conceive of an instance where a system without cyber components would be vulnerable to cyber stress. One could make a system completely resistant to cyber attack by removing all of the cyber components; however, the added security may not justify the loss in performance. Although there may be use cases where this is appropriate, this kind of complete resistance does not lend itself to quantitative measurement.

The cases that are more questionable are those that involve cyber systems and noncyber stress. Consider a cyber physical system like a power grid. It would certainly be called cyber resilience if some nodes were infected with malware and the system automatically rerouted traffic around them while they were repaired. Would it be considered cyber resilience if the same nodes were offline because of weather and the system automatically rerouted power around them while they were repaired? Consider a cyber physical system like a heavy vehicle. It would certainly be called cyber resilience if the system noticed that one of the sensors was reporting erroneous data because a cyber attack and supplied appropriate data computed through other means.[123] Would it be called cyber resilience if the same thing happened but the sensor failed for a reason unrelated to a cyber attack? There is another case. Consider a cyber attack against the cooling system of a military vehicle. The attack fools the system into believing that the engine temperature is low enough that the radiator fan is not required. This attack could allow the vehicle to overheat to the point the lubricant fails and the engine ceases. However, modern vehicles are built with very large cooling systems that only require the fan in the presence of physical stress. Without this physical stress, the cyber attack may not be manifest. Many systems are designed such that maximum capacity is significantly higher than the expected normal requirement. The overcapacity could mask the effect of a cyber attack. Should redundant capacity be considered a cyber defense?

Consider that there are sometimes important interactions between cyber and noncyber stresses and the desire for cyber, especially cyber phyiscal, systems to be tenacious in the face of both cyber and noncyber stress. As a final consideration, cyber components are often introduced into systems to improve their tenacity against noncyber stress. Exclusion of noncyber stress from the definition of cyber resilience could lead to a measurement that discounts the original purpose of the cyber components. It seems that the definition of cyber resilience must be restricted to cyber

systems, but need not be restricted to cyber stress.

4.6 Operational Definition

Although a scientific definition is not an operational definition, it is valuable to discuss how the scientific definition of cyber resilience may be measured. Three measures immediately present themselves. Since resilience in general and cyber resilience is particular describes the interaction between stress and strain, one could measure cyber resilience as the amount of cyber stress an object is able to endure and still return to the original state once the stress is removed. Béné[31] described measuring resilience in terms of cost. Finally, one could measure cyber resilience by measuring the cyberstrain or the impact on a systems key performance parameters (KPPs).

Measuring the cyber strain that a system can endure and yet still return to its original function may be the most natural way to measure cyber resilience. It is certainly the most in keeping with the way resilience is measured in material science. Consider the existence of some measurement of cyber pressure, (*e.g.*, a cyber Pascal.) If it were possible to measure the force a cyber attack, then cyber relience would be the cyber Pascals required to bring the system to its elastic limit. The problem is that there is no good method to quantitatively measure the strength of a cyber attack. There are some discreet measures of cyber attacks; however, the quantitative measurement of the strength of cyber attack is an open research topic.

Measuring resilience in terms of cost has many very attractive aspects. One clear benefit is that it would allow the cost of the implementation of a cyber resilience approach to be compared with the projected cost savings to clearly understand if the cost of implementation is justified. This approach may very well be the best final result for many commercial systems; however, the goal of this study was to measure the cyber resilience of military systems. The cost of mission failure in these circumstances is more difficult to calculate.

The final method to consider is measuring the cyber strain of a system under cyber stress. This strain may be measured by the impact to the systems KPPs over the course of a mission under cyber attack. This method would allow the quantitative measurement of the family of cyber tenacity by measuring the difference in KPPs without and with cyber stress.

Brtis[9] evaluated 23 candidates against 19 criteria and concluded that the best single metric for resiliency is the expected availability of the required capability. This was the approach taken by Smith et al.[124] and refined by Kott et al.[125] If cyber systems obey Hooke's law,[52] which is by no means guaranteed, it is possible that this might also quantitatively measure cyber stress like a spring scale.

4.7 Definition Proposal

In order to prevent the expansion of the meaning of resilience until it becomes a meaningless buzzword, it is necessary that the scientific definition of cyber resilience be restricted and focused. The definition of resilience began with the concept of jumping back or recoiling; a focused definition would center on recovery or spring over stiffness or toughness. Cybenko[86] said, "Loosely speaking, 'cyber resiliency' refers to an information processing system's ability to return to some level of desired performance after a degradation of that performance." This definition may be too focused because not all cyber systems are information processing systems. Beling et al.[94] said that resilience "is a high-level property relating to the capacity of the systems to recover from unwanted loss of function." It is not clear that the level of the property is relevant. The term loss of function seems too discrete for a quantitative measurement. Linkov and Kott[113] said, "Cyber resiliency refers to the system's ability to recover or regenerate its performance after a cyber attacks produces a degradation of its performance." This definition may needlessly restrict cyber resilience to cyber attacks. As discussed previously, the capability of a computer system to recover from physical failure could be considered cyber resilience. Also regenerate implies to construct or create a new or improved manner that expands into adaptability or perseverance.

Synthesizing these definitions by removing the unnecessary restrictions provides the following definition of cyber resilience: "The ability of a cyber system to recover from stress that causes a reduction of performance." In this definition, a cyber system is any system that employs computing technology to accomplish its purpose. This could be a traditional computing platform, a robotic platform, or a modern automobile. It is distinguished from cyber resistance because it allows for a reduction in performance where cyber resistance would not. It is distinguished from cyber persistence because resilience requires recovery where persistence does not. It is distinguished from cyber perseverance because perseverance requires recovery to an improved state.

Consider by way of example a cluster of systems supporting a website. Under normal operation, requests are distributed to various nodes all working together. Consider the same system under cyber attack. Cyber tenacity would describe the the full interaction between the impact to the operation of the system, strain, and the cyber attack, stress. The system demonstrates cyber resistance when the operation of the system is not measurably impacted while under cyber attack. This would be the case if the system were patched against the particular vulnerability that the malware exploits. The system demonstrates cyber resilience when the operation of the systems is measurably impacted during the cyber attack, but returns to normal operation when the attack is removed or nullified. This might be the case in a distributed denial of service attack. The system demonstrates cyber persistence when the operation of the is measurably impacted, but the system is able to continue to function at an acceptable but diminished level of service. This might be the case if one of the nodes is infected, the system is able to detect this, and shuts down the node. The system would demonstrate cyber resilience if it reimaged the node and brought it back into service. The system would demonstrate cyber perseverance if it discovered the attack vector and closed that vector against future attack.

4.8 Measures of Success

The following list compares the measures of success enumerated in Section 2.3 against the definition of cyber resilience presented in the previous section: *The ability of a cyber system to recover from stress that causes a reduction of performance.*

1. *A valid scientific definition is a real definition associating a word to a unique concept that may observed and measured.* This concept of resilience is real in that it may be observed and measured in the way systems react to cyber stress. This concept of resilience is unique in that it focuses on only the elastic phase of the stress strain continuum.

2. *A valid scientific definition is clear.* This definition is clear in that does not used vague words except in areas where the meaning is specific to the system but not the definition. The concepts of performance, level of performance, and degradation are left vague because these are unique to particular systems or classes of systems and this definition is meant to apply many different kinds of cyber systems.

3. *A valid scientific definition differentiates the concept from related concepts.*

By focusing on the elastic phase of the stress strain interaction, (*i.e.*, recovery of performance after unwanted degradation,) this definition differentiates itself of other aspects of stress strain interaction (*e.g.*, resistance, persistence, and perseverance.)

4. *A valid scientific definition is consistent with the historical use of the word.* As seen in Section 4.1, the historical definition of resilience describes the concept of recovering or returning to the original shape or condition after some external force has caused a change. This definition cyber resilience is consistent with the historical definition of resilience.

5. *A valid scientific definition should not contain the the means for attaining it.* This definition focuses only on the property of responding to stress elastically, and it provides no direction as to how this property might be achieved.

5. Conclusion

The recent explosion in the popularity and varying definitions of resilience have left it a panchreston. If the concept of resilience is to have any scientific significance, its meaning must be better focused. The proposed method of focusing the meaning of resilience is to understand it as part of a family of the properties, under the umbrella of tenacity, that describes the relationship between stress and strain on a system. Cyber resistance is the ability of a system to withstand stress without any perceptible reduction in performance. Cyber resilience is *the ability of a cyber system to recover from stress that causes a reduction of performance.* Cyber persistence is the ability of a system to perform at a reduced but acceptable level under stress. Cyber perseverance is the ability of a system grow in tenacity through exposure to stress. These may all be measured by the degradation of KPPs caused by the stress. There is still much work to be done to take this concept of cyber tenacity, in general, and cyber resilience, in particular, and mathematically model and quantitatively measure it.

6. References

1. Kott A, Linkov I. To improve cyber resilience, measure it. Computer. 2021;54(2):80–85.

2. Locke EA. Good definitions: the epistemological foundation of scientific progress. In: Greenberg J, editor. Organizational behavior: the state of the science; 2nd ed. Lawrence Erlbaum Associates; 2003. p. 395–425.

3. Podsakoff PM, MacKenzie SB, Podsakoff NP. Recommendations for creating better concept definitions in the organizational, behavioral, and social sciences. Organizational Research Methods. 2016;19(2):159–203.

4. Wacker JG. A theory of formal conceptual definitions: developing theory-building measurement instruments. Journal of Operations Management. 2004;22(6):629–650.

5. Hibberd FJ. What is scientific definition? Journal of Mind & Behavior. 2019;40(1):29–52.

6. Mulligan K, Scherer KR. Toward a working definition of emotion. Emotion Review. 2012;4(4):345–357.

7. Maul A. Rethinking traditional methods of survey validation. Measurement: Interdisciplinary Research and Perspectives. 2017;15(2):51–69.

8. Rossiter JR. Optimal standard measures: comment on Matthews et al.(2016). The American Psychologist. 2017;72(5):489–490.

9. Brtis J. How to think about resilience in a DOD context. Mitre Corporation; 2016 Aug. Report No.: MTR160138.

10. Cao M. Transportation resilience: a summative review on definition and connotation. In: International Conference on Automation, Mechanical Control and Computational Engineering; 2015 Apr 24–26; Ji'nan, CN. Atlantis Press; 2015. p. 1127–1132.

11. Aburn G, Gott M, Hoare K. What is resilience? An integrative review of the empirical literature. Journal of Advanced Nursing. 2016;72(5):980–1000.

12. Björck F, Henkel M, Stirna J, Zdravkovic J. Cyber resilience–fundamentals for a definition. In: Rocha A, Correia AM, Costanzo S, Reis LP, editors. New contributions in information systems and technologies; Vol. 1; 2015 Mar; Maderia, Portugal. Springer; 2015. p. 311–316.

13. Hoffman RR, Hancock PA. Measuring resilience. Human Factors. 2017;59(4):564–581.

14. Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliability Engineering & System Safety. 2016;145:47–61.

15. Spence J. Observations, anecdotes, and characters of books and men. John Murray; 1820.

16. Saxe JG. The poetical works of John Godfrey Saxe. Houghton, Mifflin and Company; 1899.

17. Gigerenzer G. A theory integration program. Decision. 2017;4(3):133–145.

18. Klein RJT, Nicholls RJ, Thomalla F. Resilience to natural hazards: how useful is this concept? Global Environmental Change Part B: Environmental Hazards. 2003;5(1):35–45.

19. Dillon J. Resilience of fibers and fabrics. Textile Research Journal. 1947;17(4):207–213.

20. Norris FH, Stevens SP, Pfefferbaum B, Wyche KF, Pfefferbaum RL. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. American Journal of Community Psychology. 2008;41(1):127–150.

21. Reid R, Botterill LC. The multiple meanings of 'resilience': an overview of the literature. Australian Journal of Public Administration. 2013;72(1):31–40.

22. Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety. 2015;141:5–9.

23. Arghandeh R, Von Meier A, Mehrmanesh L, Mili L. On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews. 2016;58:1060–1069.

24. Xue X, Wang L, Yang RJ. Exploring the science of resilience: critical review and bibliometric analysis. Natural Hazards. 2018;90(1):477–510.

25. Cottam BJ, Specking EA, Small CA, Pohl E, Parnell GS, Buchanan RK. Defining resilience for engineered systems. Canadian Center of Science and Education; 2019.

26. Robinson R. Definition. Oxford University Press; 1950.

27. Bridgman PW. The logic of modern physics. Macmillan; 1927.

28. Miller WJ. A working definition for total quality management (TQM) researchers. Journal of Quality Management. 1996;1(2):149–159.

29. Date CJ. What not how the business rules approach to application development. Addison-Wesley; 2000.

30. Patton GS, Harkins PD. War as I knew it. Houghton Mifflin Harcourt; 1995.

31. Béné C. Towards a quantifiable measure of resilience. IDS Working Papers. 2013;2013(434):1–27.

32. Seville E. Resilience: great concept but what does it mean? In: Council on competitiveness - risk intelligence and resilience workshop; University of Canterbury. Civil and Natural Resources Engineering; 2008.

33. Hussain M. Resilience: meaningless jargon or development solution. The Guardian. 2013;5.

34. Phillips FY, Chao A. Rethinking resilience: definition, context, and measure. IEEE Transactions on Engineering Management; 2022 [accessed 2023 June 7]. https://ieeexplore.ieee.org/document/9686593. 10.1109/TEM.2021.3139051.

35. Olsson L, Jerneck A, Thoren H, Persson J, O'Byrne D. Why resilience is unappealing to social science: theoretical and empirical investigations of the scientific use of resilience. Science Advances. 2015;1(4):e1400217.

36. Kerlinger FN. Foundations of behavioral research. Holt, Rinehart & Winston; 1966.

37. Boysen GA, Ebersole A. Expansion of the concept of mental disorder in the DSM-5. The Journal of Mind and Behavior. 2014;35(4):225–243.

38. Resile. In: Webster's new world dictionary of the American language (college edition). The World Publishing Co.; 1955.

39. Resile. In: McKechnie JL, editor. Webster's new twentieth century dictionary of the English language unabridged; Second ed. New World Dictionaries/Simon and Schuster; 1983.

40. Resile. In: Brown L, editor. The new shorter Oxford English dictionary on historical principles; 4 ed. Vol. 2; Oxford University Press; 1993.

41. Resile. In: Pickett JP, editor. The American heritage dictionary of the English language; Fourth ed. Houghton Mifflin Company; 2006.

42. Resilience. In: Webster's new world dictionary of the American language (college edition). The World Publishing Co.; 1955.

43. Resilience. In: Stein J, editor. The Random House college dictionary; Revised ed. Random House, Inc.; 1980.

44. Resilience. In: McKechnie JL, editor. Webster's new twentieth century dictionary of the English language unabridged; Second ed. New World Dictionaries/Simon and Schuster; 1983.

45. Resilience. In: Brown L, editor. The new shorter Oxford English dictionary on historical principles; 4 ed. Vol. 2. Oxford University Press; 1993.

46. Resilience. In: Pickett JP, editor. The American heritage dictionary of the English language; Fourth ed. Houghton Mifflin Company; 2006.

47. Resilience. In: Wilkinson KL, editor. The Merriam-Webster dictionary. Merriam-Webster, Incorporated; 2019.

48. Resilience. In: Cambridge dictionary English dictionary. Cambridge University Press; 2022.

49. Resilience. In: Rundell M, editor. Macmillan dictionary. Macmillan Education Limited; 2022.

50. Rankine W. A manual of applied mechanics. R. Griffin; 1858. (Encycl. Metropolitana, 2nd ed. vol.39).

51. Ahmmad R, Jumaat M, Bahri S, Islam AS. Ductility performance of lightweight concrete element containing massive palm shell clinker. Construction and Building Materials. 2014;63:234–241.

52. Hooke R. Lectures de potentia restitutiva, or of spring explaining the power of springing bodies. John Martyn; 2016.

53. Hoffman R. A generalized concept of resilience. Textile Research Journal. 1948;18(3):141–148.

54. Holling CS. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics. 1973;4(1):1–23.

55. Gruemm HR. Definitions of resilience. International Institute for Applied Systems Analysis; 1976. Report No.: RR-76-005.

56. Bodin P, Wiman B. Resilience and other stability concepts in ecology: notes on their origin, validity, and usefulness. ESS Bulletin. 2004;2(2):33–43.

57. Garmezy N. Vulnerability research and the issue of primary prevention. American Journal of Orthopsychiatry. 1971;41(1):101.

58. Egeland B, Carlson E, Sroufe LA. Resilience as process. Development and psychopathology. 1993;5(4):517–528.

59. Masten AS. Ordinary magic: resilience processes in development. American Psychologist. 2001;56(3):227.

60. Glantz MD, Sloboda Z. Analysis and reconceptualization of resilience. In: Glantz MD, Johnson JL, editors. Resilience and development: positive life adaptions; Springer; 2002. p. 109–126.

61. Luthar SS, Cicchetti D, Becker B. The construct of resilience: a critical evaluation and guidelines for future work. Child Development. 2000;71(3):543–562.

62. Connor KM, Davidson JR. Development of a new resilience scale: the Connor-Davidson resilience scale (CD-RISC). Depression and Anxiety. 2003;18:76–82.

63. Wald J, Taylor S, Asmundson GJ, Jang KL, Stapleton J. Literature review of concepts: psychological resiliency. British Columbia University Vancouver; 2006. Report No.: W7711-057959/A.

64. Fleming J, Ledogar RJ. Resilience, an evolving concept: a review of literature relevant to aboriginal research. Pimatisiwin. 2008;6(2):7.

65. Wildavsky AB. Searching for safety. Transaction Publishers; 1988.

66. Comfort LK. Shared risk: complex systems in seismic response. Emerald Group Publishing; 2007.

67. Adger WN. Social and ecological resilience: are they related? Progress in Human Geography. 2000;24(3):347–364.

68. Berkes F, Colding J, Folke C. Navigating social-ecological systems: building resilience for complexity and change. Cambridge University Press; 2008.

69. Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, von Winterfeldt D. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra. 2003;19(4):733–752.

70. Rose A. Defining and measuring economic resilience to disasters. Disaster Prevention and Management: An International Journal. 2004;13(4).

71. National preparedness. Office of the President (US); 2011 Mar 30. Presidential Policy Directive No.: PPD-8.

72. National Research Council. Disaster resilience: a national imperative. National Academies Press; 2012.

73. Alexander DE. Resilience and disaster risk reduction: an etymological journey. Natural Hazards and Earth System Sciences. 2013;13(11):2707–2716.

74. Southwick SM, Bonanno GA, Masten AS, Panter-Brick C, Yehuda R. Resilience definitions, theory, and challenges: interdisciplinary perspectives. European Journal of Psychotraumatology. 2014;5(1):1–14.

75. Musman S, Agbolosu-Amison S. A measurable definition of resiliency using "mission risk" as a metric. Mitre Corporation; 2014. Mitre Technical Report No.: MTR140047.

76. Larkin S, Fox-Lent C, Eisenberg DA, Trump BD, Wallace S, Chadderton C, Linkov I. Benchmarking agency and organizational practices in resilience decision making. Environment Systems and Decisions. 2015;35:185–195.

77. Building Resilience: The EU's approach. European Commission Factsheet; 2016.

78. Goldman H, McQuaid R, Picciotto J. Cyber resilience for mission assurance. In: 2011 IEEE International Conference on Technologies for Homeland Security (HST); 2011 Nov; Boston, MA. IEEE; 2011. p. 236–241.

79. Woods DD, Branlat M. Basic patterns in how adaptive systems fail. Resilience Engineering in Practice. 2011;2:1–21.

80. Partnering for cyber resilience. World Economic Forum; 2012 [accessed 2022 Mar 1]. https://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

81. Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A. Resilience metrics for cyber systems. Environment Systems and Decisions. 2013;33(4):471–476.

82. Pawlikowski E, Loverro D, Cristler T. Resiliency and disaggregated space architectures. Air Force Space Command; 2013.

83. Cureton KL, Brtis JS. Resilient systems working group. INCOSE – International Council on Systems Engineering; 2015 [accessed 2022 Jan 24]. https://www.incose.org/incose-member-resources/working-groups/analytic/resilient-systems.

84. Khan YI, Al-shaer E, Rauf U. Cyber resilience-by-construction: modeling, measuring & verifying. In: Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense; 2015 Oct 12; Denver, CO. (SafeConfig '15) Association for Computing Machinery; 2015. p. 9–14.

85. Committee on national security systems (CNNS) glossary. CNNS; 2015 Apr. CNSSI No.: 4009.

86. Cybenko G. Quantifying and measuring cyber resiliency. In: Carapezza EM, editor. Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XV; Vol. 9825; 2016 Apr 18–19; Baltimore, MD. SPIE; 2016. p. 156 – 161.

87. Baros S, Shiltz D, Jaipuria P, Hussain A, Annaswamy AM. Towards resilient cyber-physical energy systems. Active Adaptive Control Laboratory (AACL) Preprints. 2017.

88. Joint Task Force. Security and privacy controls for information systems and organizations. National Institute of Standards and Technology; 2017. Special Publication No.: 800-53 Rev. 5.

89. Clark A, Zonouz S. Cyber-physical resilience: definition and assessment metric. IEEE Transactions on Smart Grid. 2019;10(2):1671–1684.

90. Bellini E, Marrone S. Towards a novel conceptualization of cyber resilience. In: 2020 IEEE World Congress on Services (SERVICES). p. 189–196.

91. Faulkner A, Franz G, Dalling D, Layman J. Achieving federal cyber resilience. Accenture; 2020 Aug 20 [accessed 2022 Jan 24]. https://www.accenture.com/us-en/insights/us-federal-government/achieving-federal-cyber-resilience.

92. Andersson J, Grassi V, Mirandola R, Perez-Palacin D. A conceptual framework for resilience: fundamental definitions, strategies and metrics. Computing. 2021;103(4):559–588.

93. Laprie JC. From dependability to resilience. In: 38th IEEE/IFIP Int. Conf. on Dependable Systems and Networks; 2008 June 24–27; Anchorage, AK. IEEE; 2008. p. G8–G9.

94. Beling P, Horowitz B, McDermott T. Developmental test and evaluation (DTE&A) and cyberattack resilient systems. Systems Engineering Research Center; 2021 Sep. Technical Report No.: SERC-2021-TR-015.

95. Glossary. ISACA; 2022 Jan [accessed 2022 Jan 24]. https://www.isaca.org/resources/glossary.

96. Brtis J, Jackson S, Cureton K. System Resilience. Systems Engineering Body of Knowledge (SEBok); 2021.

97. Critical infrastructure security and resilience. Office of the President (US); 2013 Feb 12. Presidential Policy Directive No.: PPD-21.

98. Committee on Payments and Market Infrastructures. Cyber resilience in financial market infrastructures. Bank for International Settlements; 2014.

99. Azebbi CE. Safe, secure and prosperous: a cyber resilience strategy for Scotland. Scottish Government; 2015 Nov 18 [accessed 2022 Jan 24]. https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/.

100. DiMase D, Collier ZA, Heffner K, Linkov I. Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions. 2015;35(2):291–300.

101. Cutter SL, Ahearn JA, Amadei B, Crawford P, Eide EA, Galloway GE, Goodchild MF, Kunreuther HC, Li-Vollmer M, Schoch-Spana M, Scrimshaw SC, Stanley EM, Whitney G, Zoback ML. Disaster resilience: a national imperative. Environment: Science and Policy for Sustainable Development. 2013;55(2):25–29.

102. Dessavre D, Ramirez-Marquez J. Computational techniques for the approximation of total system resilience. In: Podofillini L, Sudret B, Stojadinovic B, Zio E, Kroger W, editors. Safety and Reliability of Complex Engineered Systems: ESREL 2015; 2015 Sep; Zurich, Switzerland. CRC Press; 2015.

103. Graubart R, Bodeau D. Cyber resilience metrics: key observations. Mitre Corporation; 2016. Report No.: AD1107819.

104. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics, measures of effectiveness, and scoring: enabling systems engineers and program managers to select the most useful assessment methods. Mitre Corporation; 2018 Sep. Report No.: MTR180314.

105. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics catalog. Mitre Corporation; 2018 Sep. Report No.: MTR180450.

106. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics and scoring in practice use case methodology and examples. Mitre Corporation; 2018 Sep. Report No.: MTR180449.

107. Markin C, Samans R. Cyber resilience playbook for public-private collaboration. World Economic Forum; 2018.

108. Carías JF, Arrizabalaga S, Labaka L, Hernantes J. Cyber resilience progression model. Applied Sciences. 2020;10(21).

109. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient systems: a systems security engineering approach. National Institute of Standards and Technology; 2021. NIST Special Publication No.: 800-160.

110. Alexeev A, Henshel DS, Levitt K, McDaniel P, Rivera B, Templeton S, Weisman M. Constructing a science of cyber-resilience for military systems. In: NATO IST-153 Workshop on Cyber Resilience; Munich, Germany. p. 23–25.

111. Deutscher SA, Bohmayr W, Asen A. Building a cyberresilient organization. BCG Perspectives. 2017.

112. Whelihan D, Vai M, Evanich N, Kwak KJ, Li J, Britton M, Frantz B, Hadcock D, Lynch M, Schafer D, DeMatteis J, Russo D. Designing agility and resilience into embedded systems. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM); IEEE; 2017. p. 249–254.

113. Linkov I, Kott A. Fundamental concepts of cyber resilience: Introduction and overview. In: Kott A, Linkov I, editors. Cyber resilience of systems and networks. Springer; 2019. p. 1–25.

114. Lindenmayer DB, Fischer J. Tackling the habitat fragmentation panchreston. Trends in Ecology & Evolution. 2007;22(3):127–132.

115. Juran JM. Juran on leadership for quality. Simon and Schuster; 2003.

116. Barbacci M, Klein M, Longstaff T, Weinstock C. Quality attributes. Software Engineering Institute, Carnegie Mellon University; 1995. Report No.: CMU/SEI-95-TR-021.

117. IEEE standard for a software quality metrics methodology. IEEE Std 1061-1992. 1993;:1–96.

118. Littlewood B, Strigini L. Software reliability and dependability: a roadmap. In: Proceedings of the Conference on the Future of Software Engineering; 2000 May 1; Limerick, Ireland. Association for Computing Machinery; 2000. p. 175–188.

119. Bishop M. What is computer security? IEEE Security & Privacy. 2003;1(1):67–69.

120. Rungger M, Tabuada P. A notion of robustness for cyber-physical systems. IEEE Transactions on Automatic Control. 2016;61(8):2108–2123.

121. Tabuada P, Caliskan SY, Rungger M, Majumdar R. Towards robustness for cyber-physical systems. IEEE Transactions on Automatic Control. 2014;59(12):3151–3163.

122. Cyber. In: Cambridge dictionary English dictionary. Cambridge University Press; 2022.

123. Shirazi H, Pickard W, Ray I, Wang H. Towards resiliency of heavy vehicles through compromised sensor data reconstruction. In: Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy; 2022 Apr 25–27; Baltimore, MD. Association for Computing Machinery; 2022. p. 276–287.

124. Smith SC, Raio S, Erbacher RF, Weisman M, Parker TW, Ellis JE. Quantitative measurement of cyber resilience: a tabletop exercise. DEVCOM Army Research Laboratory (US); 2022 Jan. Technical Report No.: ARL-TR-9380.

125. Kott A, Weisman MJ, Vandekerckhove J. Mathematical modeling of cyber resilience. In: MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM); 2022 28 Nov– 2 Dec; Rockville, MD. IEEE ComSoc; 2022. p. 849–854.

List of Symbols, Abbreviations, and Acronyms

CNNS	Committee on National Security Systems
IEEE	Institute of Electrical and Electronics Engineers
KPP	key performance parameter

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLB CI TECH LIB
1 (PDF)	OUSD(R&E) C MACIAG
1 (PDF)	DEVCOM ARL FCDD RLA ND S SMITH