Introducing Hilbert Space and Quantum Cognition to Cyber Security Risk Management

Fariborz Farahmand, *Senior Member, IEEE*

Abstract—The existing computational cognitive models in cyber security risk management have major limitations in the analysis of cyber security behaviors. To address this issue, we introduce Hilbert space and quantum cognition to cyber security risk management. We compare some key axioms and definitions of classical cognition and quantum cognition. We provide examples on how some unique principles of Hilbert space and quantum cognition such as compatibility can help with the event representation, and capturing cognitive biases that are not possible with classical probability. We shed light on how the mathematical formalism of quantum probability can model the observed deviations from the classicality in human reasoning. We also shed light on how quantum cognition can contribute to the science and practice of cyber security. We argue that Hilbert space and quantum cognition can reconcile violations of classical probability theory in cyber security risk management with a formal theory, and examine whether it is possible to express formally some of the key heuristics in cyber security behaviors.

Index Terms—Cyber security, Hilbert space, human behavior, quantum cognition, quantum mechanics, risk management

1 Introduction

THE impracticality of the existing cyber security risk models, in capturing cyber security behaviors, has been discussed at the national level. "Many current security controls offer limited or undocumented efficacy, place a burdensome workload on administrators and authorized users, or rely on unrealistic assumptions about the environment or user behavior. Current methods fall short of realistically integrating human factors into experiments and accurately quantifying them as a security variable to be tested" [9]. In developing system design methods to incorporate privacy desires and requirements, "privacy lacks models that provide quantifiable methods for describing risk" [10].

We argue that these issues mainly have been caused by the simplistic assumptions about human behavior, and the limitations of the existing computational cognitive models in cyber security risk management. For example, a human adversary is considered as a rational agent who always obeys the axioms of expected utility theory [8] and classical probability [5]. However, the reality is that adversary could be intelligent, but highly irrational, as defined in expected utility theory, and his/her intuitive judgments frequently violate these axioms.

Similar to 1920s that many findings that seemed paradoxical from the classical point of view led physicists to develop quantum physics, we argue that the classical probability theory is too limited to fully explain various cyber security behaviors. That is, we need alternatives for classical probability and cognitive assessments to realistically capture cyber security behaviors.

• *The author is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Klaus Advanced Computing Building, 266 Ferst Drive, Atlanta 30332-0765, Georgia. E-mail: fariborz@ece.gatech.edu.*

Manuscript received 29 Sept. 2019; accepted 30 Dec. 2019. Date of publication 3 Jan. 2020; date of current version 27 Jan. 2020.
(Corresponding author: Fariborz Farahmand.)
Recommended for acceptance by J. Hughes.
Digital Object Identifier no. 10.1109/LOCS.2019.2963875

2 Introducing Hilbert Space and Quantum Cognition

We propose that cyber security research can benefit from applying the mathematical formalism of Hilbert space and quantum cognition to address the deficiencies of classical human cognition in human reasoning. Here, we adapt cases and examples from quantum cognition, [1], [2] and explain how the unique features of quantum cognition provide a more practical approach than classical probability theory to cyber security risk management. Here are couple of examples.

2.1 Hilbert Space

Quantum cognition uses Hilbert space vs. Kolmogorov axioms of probability [5] that are commonly used in cyber security risk management. In quantum cognition, H is a vector space over the set of complex numbers, which we call a complex Hilbert space. That is, the elements of a Hilbert space are vectors which include a set of real numbers.

Mathematically, Hilbert space is composed of abstract points $\mathbf{X}$. A point in $\mathbf{X}$ is represented by a $ket|X\rangle$, which is a vector [2]. Any pair of vectors can be added, or multiplied to generate another vector in the same space. The $ket|X\rangle$, corresponds to a $N \times 1$ matrix.

Hilbert space has the advantage of capturing entire concepts in one single space. Alternatively, the classical probability approaches require an associated sample space to capture each concept. Hilbert space graphically demonstrates behaviors with vectors, and can describe the influence of contexts on decisions and behaviors.

2.2 Subspace

The events in quantum probability theory are defined as subspaces instead of sets. Subspaces are geometric objects in vectors spaces, and they correspond to projectors which establish relationships between the state vectors and subspaces [1], [2]. A *projector* maps the input into output. Such process is called *projecting*, and the output is called *projection*. The probability assigned to an event equals the squared length of the projection. The probability function of an event in quantum cognition is a projection of the state on the subspace. For example, if we have a unit length state vector S in the Hilbert space, the probability of the event is represented by $\|P_{event}.S\|^2$. That is, the concept of "space" is quite different in classical probability and quantum cognition. In classical probability, a single sample space is a complete and exhaustive description of all events, whereas in quantum theory, subspaces (multiple sample spaces) describe different types of events.

Simply speaking, we can adapt the von Neumann's definition of events in quantum mechanics [7] to another definition based on subspaces of a vector space. With adaptation, we use a state vector S that represents the state of the cognitive system, instead of using a function P to identify probabilities for events. We also use a state vector S that represents the state of the cognitive system, and a projector. See Table 1 for a comparison of classical cognition and quantum cognition.

3 Compatibility and Event Representation in Hilbert Space

Cognitive measures can disturb each other, however classical probability cannot capture such disturbance. Here is a simple, tangible example. Assume you and your family are discussing your housing preference with a real estate agent. In scenario 1, the agent ask you directly the type of home you would like to buy, and you respond with a specific preference. In scenario 2, however the agent first ask the same question from your family, and then ask you about your

TABLE 1
Comparison of Some Key Axioms and Definitions of Classical Cognition and Quantum Cognition, Based on Classical Probability Theory and Quantum Theory, Respectively (Adapted and Modified From Bruza *et al.* [1]).

Classical cognition		Quantum cognition	
i.	Events are subsets of a universal set U. Events, such as A and B, are subsets of U.	i.	Events are subspaces of a Hilbert space $\mathcal{H}$. Events, such as A and B, correspond to subspaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively of $\mathcal{H}$. Associated with these subspaces are projectors $P(A)$ and $P(B)$.
ii.	A function P represents the state of the cognitive system. Function P is defined on the subsets in U, and the probability of an event A equals $P(A)$.	ii.	If projectors $P(A)$ and $P(B)$ are commutative, that is, $P_AP_B = P_BP_A$, then the events A and B are compatible. Otherwise, they are incompatible.
iii.	$P(A) \geq 0$, and $P(U) = 1$.	iii.	The state of the cognitive system is represented by a unit length vector S in the vector space, and the probability of event A equals $\|P_A.S\|^2$.
iv.	If $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.	iv.	$\|P_A.S\|^2 \geq 0$ and $\|P_{\mathcal{H}}.S\|^2 = 1$. If $P_AP_B = 0$, then $\|(P_A + P_B).S\|^2 = \|P_A.S\|^2 + \|P_B.S\|^2$
v.	Law of total probability: $P(B) = P(A \cap B) + P(\not\sim A \cap B)$.	v.	Violation of the law of total probability: $\|P_B.S\|^2 \neq \|P_B.P_A.S\|^2 + \|P_B.P_{\not\sim A}S\|^2$.

preference. It is highly likely that the change of order of questions in the scenario 1 and 2 influence your preference. However, such influence cannot be captured by classical probability, as classical probability assumes events are compatible and commutative. That is, for the events A and B: $A \cap B = B \cap A$, and $P_AP_B = P_BP_A$.

Similarly, physicists have different ways of describing "relations between observables" [4] in nature and events that are mutually incompatible but equally valid and together necessary for a complete description. For example, in physics position and momentum are complementary ways of describing the state of particles. In fact, this is not unique to physics. In the world of economics, price and derivation are complementary ways of describing the value of a stock option. In human analysis of events, this corresponds to consideration of different perspectives or different points of view for answering questions. Such as jurisprudence, when a juror needs to view evidence from a prosecutor's point of view and then view the evidence from a defense point of view and it is not possible for him/her to hold these two incompatible views in mind at the same time.

In quantum cognition, an event refers to a possible answer to a question about features chosen from a common basis. For example, the answer "yes" to a question is one event, and the answer "no" to the same question is the complementary event. Another important feature of quantum cognition is that each event is represented by a subspace of the vector space, and each subspace has a projector that is used to evaluate the event.

In quantum cognition, in contrast to classical probability, the events A and B are not necessarily commutative. As such, their conjunction may not exist. Instead, quantum theory uses a more general concept of compatibility. That is, questions can be represented as incompatible thus allowing for one question to disturb the answer to another. Quantum theory allows for both compatible and incompatible measurements whereas classical probability theory assumes all measurements are compatible. Compatibility implies that measurements A and B can be accessed simultaneously or sequentially without interfering with each other. Consequently, incompatibility implies that A and B cannot be accessed simultaneously.

Formally, in quantum theory a sequence of two events A and B, denoted by AB is represented by the sequence of projectors P_BP_A. If the projectors commute, $P_AP_B = P_BP_A$, then the product of the two projectors corresponds to the subspace $A \cap B$, that is $P_BP_A = P(A \cap B) = P_AP_B$, and the events A and B are called compatible. Similarly, if the projectors do not commute, that is $P_BP_A \neq P_AP_B$, their product is not a projector, and the events are not called compatible. In such case, we need to evaluate the sequence using the P_BP_A-operating from right to left, first projection on A with P_A and then project on B with P_B. In summary, in classical probability $P_AP_{B|A} = P_BP_{A|B}$. However, since commutative property does not hold for quantum theory $P_AP_{B|A} \neq P_BP_{A|B}$ occurs when events are incompatible [3].

The concept of incompatibility can be applied using a vector space representation of knowledge—the same vector space can be represented by many different sets of basis vectors (corresponding to different sets of feature patterns), and the same exact state (vector) can be defined by different sets of basis vectors. Each (orthonormal) set of basis vectors corresponds to a description of the situation with a particular set of features and their combinations. But, different sets of basis vectors correspond to different descriptions, with different sets of features and combinations, representing complementary ways of thinking about events.

In the following sections, we shed light on the applications of quantum cognition in cyber security risk management.

4 Applying Quantum Cognition to Cyber Security Risk Management

In the context of cybersecurity, risk refers to the expected likelihood and consequences of threats or attacks on cyber assets. Quantum cognition can improve cyber security risk management in different ways, as described below. The formalism of quantum mechanics, by capturing the cognitive limitations that influence the assessment of probabilities, can contribute to addressing the above mentioned issues in analysis of cyber security behaviors. Cyber security risk management models are based on classical probability theory. It is possible to replace the classical probability theory in these models with the projective geometric structure of the Hilbert space. The following simplified example, shows the application of compatibility and Hilbert space in capturing conjunction fallacy, a well-documented cognitive bias.

4.1 A Simplified Example

Conjunction fallacy is an example of the cognitive biases that could be caused by the representativeness heuristic (a mental shortcut). In the representativeness heuristic, the probability that, for example Bob is a hacker is assessed by the degree to which he is representative of, or similar to, the stereotype of hackers.

Classical probability theory does not consider this heuristic, instead it considers events as the subsets of a single sample space. It also considers that the probability of the conjunction of events can never exceed the probability of one of its components. That is,

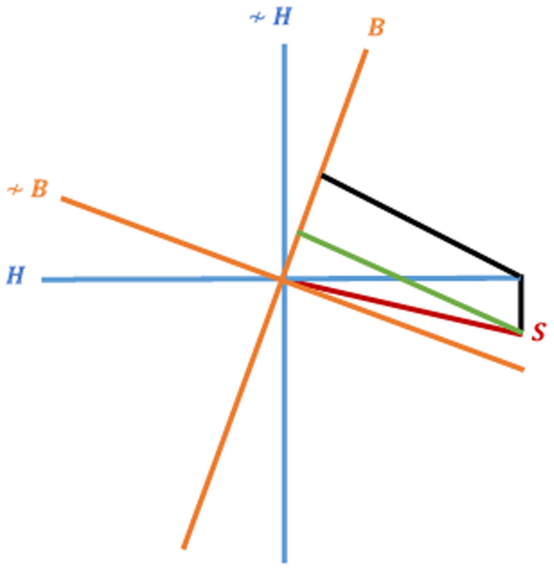

Fig. 1. Application of quantum theory to the conjunction fallacy paradigm. "Bob is a skilled hacker", represented by "$\mathbf{B}$" vs. $\mathbf{H}$: "Bob is a skilled hacker, and member of group "$\mathbf{H}$". $\mathbf{S}$ is the decision maker's cognitive state (adapted and modified from Bruza *et al.* [1]).

$P(A) > P(A \cap B)$ is impossible. However, violation of this law of classical probability, called the conjunction fallacy, has been known, starting over three decades ago (e.g., [11]). To better understand this heuristic, and how quantum cognition can help to capture it let us assume the following incident has been reported to a special agent in charge of a cybercrime investigation, and/or to a defender in an attacker/defender interaction:

"Bob" has been identified as the suspect of exploiting a zero-day vulnerability. Exploiting such a vulnerability often has been observed from the members of a famous hacking group called "H". Then, which of the following scenarios seem more probable?

1. Bob is a skilled hacker.
2. Bob is a skilled hacker, and member of group "H".

Intuitively speaking, the scenario 2 could be perceived more probable by the investigator, and/or by the defender. However, according to classical probability theory, the probability that two events occurring at the same point in time (i.e., scenario 2) can never exceed the probability of one of its constituent events (i.e., scenario 1). Here is a simplified explanation of how quantum cognition can help address this issue. In our example, let us assume scenario 1, Bob is a skilled hacker is represented by $\mathbf{B}$, and scenario 2, Bob is a member of group "H", is represented by $\mathbf{H}$ in Fig. 1. This Figure illustrates the application of incompatibility principal to the conjunction fallacy paradigm in these scenarios. The H perspective is represented as a two dimensional vector space. The blue axis H corresponds to the scenario 2, and $\sim\mathbf{H}$ corresponds to the skilled hacker is not member of group H.

Similarly, the perspective of Bob being a skilled hacker ($\mathbf{B}$), or not ($\sim\mathbf{B}$) can be can be shown by the same two dimensional vector space, but with rotated axes (the brown axes). At first, decision maker's cognitive state is shown by the red vector S which lies between the two axes.

Here, the incompatibility between the scenarios 1 and 2 can explain the conjunction fallacy. As shown in Fig. 1, assume we consider scenario 1, i.e., the event that Bob is a skilled hacker. The probability of such event is shown by the green projection–a short projection that shows a low probability. Let us consider the probability of the conjunction of events, that is, if Bob is both a skilled hacker and Bob is a member of group "$\mathbf{H}$" ($\mathbf{H}$ and $\mathbf{B}$). Since $\mathbf{H}$ and $\mathbf{B}$ are incompatible, $\mathbf{H}$ and $\mathbf{B}$ need to be considered sequentially, i.e., $\mathbf{H}$ and then $\mathbf{B}$. Precisely, the probability that two events occurring is determined by first projecting the state $\mathbf{S}$ onto the axis H, and then projecting this result onto the axis B. Fig. 1 shows the results of this two-step sequence of projections being longer than the projection of the single event $\mathbf{B}$.

5 The Expected Impact of Quantum Cognition on Cyber Security

Quantum cognition can impact both the practice and the science of cyber security.

5.1 Practice of Cyber Security

Quantum cognition can contribute to establishing effective mental models for understanding and tracking the adversaries' intent, capability, and decision process. Applying the principles of quantum mechanics can help developing an accurate and dynamic determination of the likelihood of the exploitation of the vulnerabilities. This new capability would enhance the ability to understand and cope in an imperfect information environment.

Cyber security community can apply quantum cognition to more realistically capture cyber security behaviors because: 1) There are many cognitive biases, and well-established empirical findings in cyber security research that are hard to reconcile with classic probability principles, and 2) These same findings have natural and straightforward explanations with quantum principles. In cyber security, probabilistic assessment is often strongly context and order dependent, individual states can be superposition states (that are impossible to associate with specific values), and composite systems can be entangled (they cannot be decomposed into their subsystems). All these characteristics appear perplexing from a classical perspective.

5.2 Science of Cyber Security

The first requirement of the science of cyber security is that models be "expressed in an appropriate rigorous formalism" [6]. Quantum cognition can address this need by formal capturing of biases and heuristics in cyber security risk management. It reconciles violations of classical probability theory in cyber security risk management with a formal theory and examines whether it is possible to express formally some of the key heuristics in decision-making. That is, based on the mathematical foundations of quantum mechanics, quantum cognition formalizes assigning probabilities of exploitations of vulnerabilities to observables. Quantum cognition can make this formalization by taking a geometric approach to assess probability of exploitations.

Quantum cognition, by corresponding events to different subspaces and computing probabilities by projections to these subspaces, provides a formal, accurate, and powerful account of cognitive processes of attacker/defender interactions in cyber security risk management. Additionally, quantum cognition can bridge three cultures of scholarship and research: cyber security, quantum mechanics, and cognitive science. This can lead to the mathematical translation of the findings of the cognitive science into formal models of dynamic cyber security risk management.

Acknowledgments

This research was supported by the National Science Foundation under award number 1544090.

References

[1] P. D. Bruza, Z. Wang, and J. R. Busemeyer, "Quantum cognition: A new theoretical approach to psychology," *Trends Cogn. Sci.*, vol. 19, no. 7, pp. 383–393, 2015.

[2] J. R. Busemeyer and P. D. Bruza, *Quantum Models of Cognition and Decision*. Cambridge, UK: Cambridge Univ. Press, 2014.

[3] J. R. Busemeyer and Z. Wang, "Hilbert space multidimensional theory," *Psycholo. Rev.*, vol. 125, no. 4, pp. 572–591, 2018.
[4] R. I. G. Hughes, *The Structure and Interpretation of Quantum Mechanics*, Cambridge, MA, USA: Harvard Univ. Press, 1989.
[5] A. N. Kolmogorov, *Foundations of the Theory of Probability*, Vermont, United States: Chelsea Publishing, 1956.
[6] A. Kott, "Towards fundamental science of cyber security," *Network Sci. Cybersecur.*, Berlin, Germany: Springer, 2014, pp. 1–13.
[7] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton, New Jersey, USA: Princeton Univ. Press, 1955.
[8] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton, New Jersey, USA: Princeton Univ. Press, 1953.
[9] National science and technology council, federal cybersecurity research and development strategic plan, 2016. [Online]. Available: https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf
[10] National science and technology council, national privacy research strategy, 2016. [Online]. Available: https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf
[11] A. Tversky, and D. Kahneman, "Extensional versus intuitive reasoning: the conjunction fallacy in probability judgment," *Psychol. Rev.*, vol. 90, no. 4, pp. 293–315, 1983.