Modelling Cybersecurity Systems as a Quantum Dynamical System: A Mathematical Structural Deep Learning Approach

Radhakrishnan Venkatesan
MNC, India

Abstract

Current practice of Cybersecurity is still mainly qualitative and not highly Quantitative. Though there is lots of data, logs, events, models, etc., Cybersecurity is still quantified with a limited set of parameters and not considered in full sense as a dynamic system. By understanding that the system is a flow of electrons and photons in a defined manner, I would like to incorporate the key ideas that were proposed for Dynamic Systems to be inbuilt into the Cybersecurity processes. Further by creating the necessary models of the flow we can use the Quantum tools to analyse it. Then it can be studied by the AI models in the fourier space as well as in the Deep Learning space to bring in real-time value in addition to the Cyber Threats and Threat actors.

1. Introduction

During my professional career spanning multiple roles of CyberSecurity as an End-User, Consultant, Auditor, Operations personnel, The researcher noted that though CyberSecurity is indispensable aspects of Business Goals, it still lacks the quantificational aspects. Hence both the processes, controls and residual aspects are not met with like a normal dynamical system. Many research works have happened in the last century in the Dynamical Systems including the Quantum Mechanical Systems. As CyberSecurity is the dynamics of secure information flow, we can incorporate these best practices into the CyberSecurity Domain. Some of the areas of Dynamical Systems and Mathematical Physics that can be used in the Domain of Cybersecurity include:

- Group Theory and Matrix – Cybersecurity Group Theory with the Dirac Spins Generated Using C, I, A Triad
- Potential Theory – Controls are Positive Potential and Risks are Negative Potential. Hence there will always be a flow of potential.
- Hodge Theory and Homology Concepts can be incorporated into the Cybersecurity Practices – Cybersecurity Quantum Topology.

Further analysing the data using the CyberSecurity L-functions and Laplacian based on the Group Representation. This could be the source of the AI Models training.

2. Current State of Cybersecurity Practices

Cybersecurity as a Profession is both processes based and technical or tools based. There are Governance Models, Technical standards as well as different sets of tools for various functions of the entire Cybersecutity processes. In my understanding the breadth and domains of Cybersecurity management covers:

- GRC and Processes.
- SOC and Threat / Vulnerability Management.t
- Innovation in Cybersecurity.
- Audit and support.
- Operational Cybersecurity.

Based on the size and scope of the Organization, this practice is rolled out as well as aligned with the Organizational Roles / Responsibilities.

The author has presented an initial work on Dynamical Systems into the business domain at the DIS Conference, 2024 in Greece and wanted to extend it to the Cybersecurity domain as well. The key reference to the Dynamical Systems concepts can be found in the work of Arrowsmith [1] which can be extended to any discrete or continuous dynamical systems. One of the earliest works on the Quantum mechanics is the work of Feynman [2].

Further the most comprehensive work on the analysis is the work of Whittaker [3]. The author has explored various sources of mathematical work to explore various areas of research namely, Scattering Theory[4], Modular Forms [5], Maass Forms [6], Picard Modular Surfaces [7], Quantum Groups [8], Lie Groups [9], Symplectic Groups [10], Trace Formula [11], Hecke Operators [12] to apply the same in the Cybersecurity domain. The practical implementation of the Mathematical Dynamical Systems can be found in these references [13] till [22].

 | DOI: 10.20533/jitst.2046.3723.2024.0107

3. Shortcomings and the need for a different approach

In my work experience as well as on my observations, there are multiple shortcomings in the current rollout of the Cybersecurity processes which needs a holistic attention for improvements. Some of the urgent needs that I would like to include are the below:

- Lack of Understanding of the Cybersecurity professionals on the Mathematical / Physical tools to quantify the work.
- Lack of Understanding in the Cybersecurity professionals on the Programming Domain to holistically understand the risks.
- Nonunderstanding in the Non-Cybersecurity Domains in the Corporate on the working of the Cybersecurity practices.
- Audit and Controls team are mainly Process based with not having adequate technical or mathematical expertise.
- Availability of multiple sets of tools and no standard way of configuring it and managing it when compared to the tools available in other domains.
- Lack of available resources in the senior positions, young resources seem to grow quick in the career without a solid understanding of the Criticality of the Domain.
- Implementation of the Cybersecurity frameworks in silos based on Risk Rating which is highly judgemental.
- Lack of usage of the AI Tools in critical areas other than UEBA – Behavioural Analysis and SOC Related activities.
- Cybersecurity auditors are taken mainly with the CISA qualifications which mainly focusses on the Process expertise and not on the deep expertise that is required for the Domain. This contrasts with the Domain Expertise tested in ACCA or CPA or similar standards. The Certified Accountants with a CISA can start performing IT Audits without much expertise in the area. CISA is just one multiple choice exam to get the certificate and so is the other Certifications in the field.
- Lack of Innovation in Cybersecurity in most of the Organization as the Cybersecurity team have limited coding / development skills most of the tools is outsourced from the third-party vendors.

There are some key shortcomings in the Domain of Cybersecurity innovations within the Organization:

- No Signal processing approach to Cybersecurity though the data flows is a combination of electrons and photons.
- The Cybersecurity Department does not have experts in either Coding or in dynamics or mathematical sciences.
- DevSecOps management is still through the vendor configurations or through the Opensource tools.
- The cybersecurity team has only limited knowledge on the Usage of AI or ML / DL into their domains. Further expertise in creating the models internally for the Cybersecurity or Information flow domain is still lacking.
- Data Visualization is basic. There is no visualization of data / logs in the form of dynamic vectors or dynamical systems. This is one of the key areas of concerns that needs to be addressed.

It is possible to go on adding multiple drawbacks but the point to be understood is that there is a need to revamp the field so that Cybersecurity threats are addressed holistically.

4. Approach in the Cybersecurity domain through the System Dynamics perspective

Cybersecurity as a domain in the Organization is quite complex and links most of the other departments in the firm. One of the key areas of focus of Cybersecurity is the protection of the Flow of Business Information across the Firm. This is currently done in silos based on the Priority that is defined and reviewed in the way it suits the firm. There is no standard way which says that all the Information Flow needs to be controlled, checked, and reviewed for CIA Principles (see Figure 1).

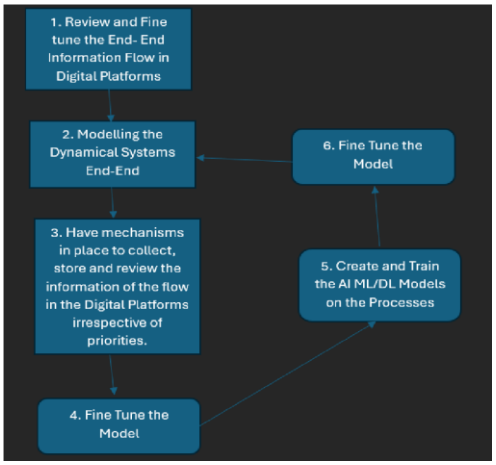

Figure 1. Fine Tune the Model

 | DOI: 10.20533/jitst.2046.3723.2024.0107

The proposed challenges can be addressed in some of these ways:

- Laying out the flow of Information end within the Organization.
- Modelling the flow and variance through Mathematical and Physical processes.
- Have mechanisms in place to collect, store and review the information of the flow in the Digital Platforms irrespective of priorities.
- Fine Tune the Model.
- Create and Train the AI ML/DL Models on the Processes.
- Fine Tune the Model again to bring in the improvements.

First Step

The first step in the whole process is the documentation of the information flow as well as the tools which drive the same. In the real scenario, the different tools available run in silos and may/may not have the right data capture enabled to monitor the flow. Further in most of the real cases if two systems are interacting the logs are dispersed across which needs to be collated / reviewed in solos to come out with an intelligence. Even if there is a centralized log management or collation, it has multiple challenges such as lack of asset inventory, configuration mismatches, team technical expertise and dependent on the third part vendors, etc.

Second Step

The Second step is critical step that needs to be addressed in multiple ways based on the expertise of the personnel in understanding any dynamical systems through the engineering lens. Few of the approaches that can be followed are documented here:

- Model the Information flow systems as a set of Discrete groups and the corresponding transformation. The way this can be modelled is based on the workflow and standard way of using the systems. If there is a deviation noted in the geometry of the groups that can be analysed for improvements. The areas of Mathematical / Physical sciences that can support here includes:
  - Groups and Symmetric Spaces o Matrix Analysis and Linear Systems o Creating the necessary differential equations of the underlying groups and manifolds.
- Model the Information flow systems as the flow of fields using the customized Cybersecurity Dirac or Other operators. The CIA Triad can be thought of operators aiding the positive flow and the inherent and other threats that emanate from the Threat Intelligence system as the negative flow. The areas of Mathematical / Physical sciences that can support here includes:
  - Quantum Mechanical Dynamics of Photons / Electrons with customized Operators specific to Cybersecurity / controls landscape.
  - Quantum Distributions and Operators.
  - Usage of available Operators from the Schrödinger and Dirac theories.
- Model the Information flow systems as a dynamic of multiple random distributions of information. Analyze and train the behaviour of such a pattern. The areas of Mathematical / Physical sciences that can support here includes:
  - Information Geometry.
  - Random Distributions and change of the distribution specific to the Information flows.
  - Pattern analysis.
- Model the Information flow systems as a flow in a Hyperbolic Geometry over time and use the necessary models to study the flow of information and associated potentials. The areas of Mathematical / Physical sciences that can support here includes:
  - Hyperbolic Geometry of Information flow and mapping it.
  - Complex analysis.
  - Upper Half plane, Poincare Disk and Simplistic flow of information.
  - Analysis of flow in the Riemannian Sphere.
  - Hodge analysis.
  - Mirror Symmetry.
- Model the Information flow systems in the Signal and Frequency Domain with the various integral transforms. The areas of Mathematical / Physical sciences that can support here includes:
  - Fourier and Laplace transform the flow by analysing the potential mismatches with the optimal bandwidth.
  - Integral transforms of the flow using the Henkel, Bessel and other operators.
  - Frequencies in the Upper Half Plan domain.
  - Boundary value analysis
  - Spectral analysis.
- Model the Information flow systems in the sense of Number theoretic approaches and fields. The areas of Mathematical / Physical sciences that can support here includes:

 | DOI: 10.20533/jitst.2046.3723.2024.0107

- Developing the specific L-Functions for the Cybersecurity information flows pertaining to the Organization
- Multiple Zeta flow analysis
- Identifying the group of Elliptic Functions and the Modular forms for the flow of information and the variations from the flows.
- Based on the CIA Triad, the analysis can be performed in the different Fields and Prime factors as per the Organization scores.

As discussed above, we can create multiple Fuchsian groups in-alignment with the Quantum Groups Models based on the Organizational needs and dynamics. These can be understood as a Complex Vector Matrix cycled around Confidentiality, Integrity, and Availability (adding anything else which may suit the need).

When the Groups are created then the Algebra related to these groups can be defined which assists in the various mathematical operations on these groups. Based on the Algebra, the dynamics of the Groups can be studied in these scenarios:

- Creating Dynamical Model.
- Categorizing the Potential flow.
- Equi distribution or Distribution of the points in the Topological spaces.
- Torsion or Deviation of the Points monitoring.

There is no limit in the way or ideas to study these dynamic objects. Once we identify the required pattern, we can use the standard analysis to check the deviation or use AI / ML models to filter the deviations. In critical IT / Cyber Infrastructure such as SCADA, Manufacturing systems, Telecom, Hospital., etc it is a need to understand the dynamics effectively by considering it in sync with the other business requirements.

Third Step

In the third step, which is one of the most important steps, the following activities are performed:

- Collection of Information and Cybersecurity related data through conventional means. Maybe there can be processes to enhance the data as well.
- Conversion of the data into the Dynamical systems data through the various options proposed in the step 2. It can be one or more of the same. In this way, we can have the data enriched which can be studied in the Dynamical space.
- In the next step we can have options to convert the final data into the original data type or in the enhanced data type through the various visualization techniques.

Fourth Step

In the fourth step, we can do the enhancement of the model, based on the data collected and analysed.

Furthermore, steps, the data is fed to the AI / ML Systems to study and fine tune the mode. This is based on the steps proposed in the Section 5. Once the mode is trained it can be used to run the entire process. It should be noted that every stage is a part of the cyclic process which needs to be regularly reviewed, updated and taken care of with the changing dynamics and the environments around it.

5. Revised Approach in the AI/ML in Cybersecurity domain

Based on the Groups and Operations created on the basic Algebra of the CyberSecurity systems, AI Models can be generated on these parameters:

- Using ML and DL based on the parameters of the CyberSecurity Groups.
- Real-time analysis of the Generated data to correlate with the Model parameters.
- Exception reports can be generated in real-time on the deviation rate specified as per the requirements.

AI Models can be generated for both DL and Reinforcement Learning as we have a well-defined base matrix and data defined to move around in space and time. Further there is no dearth in the presence of data as there are lots of Logs/Events generated in the CyberSecurity systems. The models can be generated using the Fourier Based AI Models to identify the pattern in the Signal space.

It should be noted there is no need for a complete revamp of the AI Models as we can use the existing models available in the market, fine-tune, learn the parameters and proceed with the testing. Maybe if we identify anything new in the Dynamics of Cybersecurity which needs to create a completely new AI Model that can be addressed. However, there are great models and programming platforms available in the market which can assist in the development of the AI Pipelines for the Cybersecurity Dynamics. Another area that needs to be understood is the requirement of Cloud amd Big Data storage and processing of huge amount of data that need to be consumed by the AI Models. Where needed this can work in sync with the other generic AI Solutions such as UEBA to provide the value benefits.

 | DOI: 10.20533/jitst.2046.3723.2024.0107

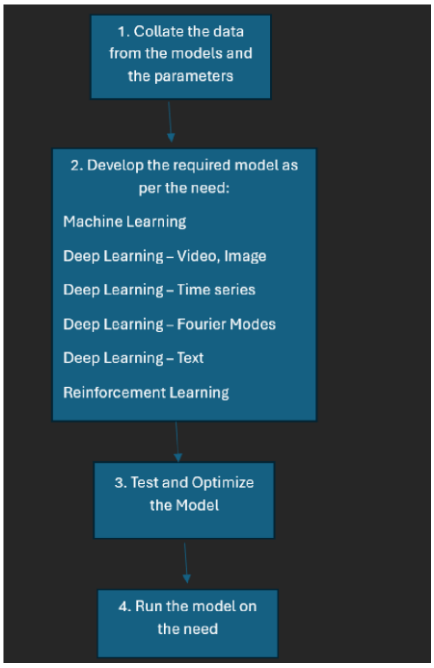

Figure 2. Available Options

In certain cases, we can use the language models to understand the dynamics of the business rules and the mismatches / alignments.

6. Way Forward

Following the above conventional approaches, we can holistically understand the flow of the Information and analyze the impact of threats of variances in the flow. By combining the best dynamic flow principles and the AI Domain models it will help the Organization to mitigate the risks real-time and gives the management the flow of the Dynamical system as well as the bottle necks / Saddle Points.

Figure 3. Sample Dynamical Systems of the Business flow / Cybersecurity controls generated using the data conversion

Once we identify the points of concerns, we can focus on protecting it effectively in a Cost / Benefit manner to reduce / transfer the risk.

7. Conclusion

By taking the best practices being developed over a century in Dynamical Systems by the Legends of Mathematics and Physics, we can incorporate those best practices to another less understood Dynamical System namely CyberSecurity. Information flow and the corresponding Cybersecurity Threats / Risks once categorized into the mathematical flow, lots of problems can be analyzed and addressed. Some of the problems include:

- Privacy controls
- Enhanced business controls
- Optimization of resources
- Wastage of the underlying assets
- Threats, vulnerabilities and risks controls
- Mathematical savvy enterprise
- Manufacturing, SCADA and other critical infrastructures can be protected effectively

Adding Intelligence and AI Models over the plethora of the data available we can perform wonders to understand Cybersecurity, which is still qualitative and less understood for any proactive preparation of attacks as well as threats. There is a need to develop the next generation on the understanding that the Information flow and Cybersecurity are complex systems which needs to be tackled with outofthe box thinking rather than in a qualitative ad hoc template. In this way we can prepare the Organization to face future challenges and threats to the Information flow effectively and with the best-in-class tools. Further there is a need to bringing visualization tools to the Cybersecurity information flow in-alignment with the policies and procedures.

8. References

[1] Arrowsmith, D. K. and Place, C. M. (1990). An Introduction to Dynamical Systems. Cambridge University Press.

[2] Feynman, R. P. (2010). Quantum Mechanics and Path Integral. Dover Publications Inc.

[3] Whittaker, E. T. and Watson, G. N. (1996). A Course of Modern Analysis. Cambridge University Press. DOI: 10.1017/CBO9780511608759.

[4] Lax, P. D. and Phillips, R. S. (1977). Scattering Theory for Automorphic Functions. (AM-87), Volume 87. Princeton University Press. DOI: 10.1515/9781400881567.

[5] Sarnak, P. (1990). Some applications of modular forms - Cambridge University Press. DOI: 10.1017/CBO9780511895593.

 | DOI: 10.20533/jitst.2046.3723.2024.0107

[6] Bringmann, K., Folsom, A., and Ono, K. (2017). Harmonic Maass Forms and Mock Modular Forms Theory and Applications. American Mathematical Society.

[7] Robert Janglands, P. and Dinakar Ramakrishnan. (1998). The Zeta Functions of Picard Modular Surfaces. American Mathematical Society.

[8] Haboush, W. and Parshall, B. (1994). Algebraic Groups and Their Generalizations Quantum and Infinite-Dimensional Methods. American Mathematical Society.

[9] Varopoulos, N. Th. (2020). Potential Theory and Geometry on Lie Groups (New Mathematical Monographs, Series Number 38). Cambridge University Press. DOI: 10.1017/9781139567718.

[10] Omeara, O. T. (1978). Symplectic Groups. Mathematical Surveys and Monographs. American Mathematical Society. DOI: 10.1090/surv/016.

[11] Knightly, A. and Li, C. (2013). Kuznetsovs trace formula and the Hecke eigenvalues of Maass forms. American Mathematical Society. DOI: 10.1090/S0065-9266-2012-00673-3.

[12] Knightly, A. and Li, C. (2006). Traces of Hecke operators. American Mathematical Society.

[13] Bump, D. and Goldfeld, D. (2006). Multiple Dirichlet Series, Automorphic Forms, and Analytic Number Theory. American Mathematical Society.

[14] Wallach, N. R. (2018). Symplectic geometry and Fourier analysis. Dover Publications Inc.

[15] Luong, B.. (2009). Fourier analysis on finite Abelian groups - Springer. DOI: 10.1007/978-0-8176-4916-6.

[16] Donagi, R. Y. and Wendland, K. (2008). From Hodge Theory to Integrability and TQFT tt-star-geometry. American Mathematical Society.

[16] Deligne, P. (1982). Hodge Cycles, Motives, and Shimura Varieties. Springer. DOI:10.1007/978-3-540-38955-2.

[17] Mitrea, D. (2016). The Hodge-Laplacian Boundary Value Problems on Riemannian Manifolds. De Gruyter Studies in Mathematics. DOI: 10.1515/9783110484380.

[19] Akin, E. (1993). The General Topology of Dynamical Systems. American Mathematical Society.

[20] Silverman, J. H. (2007). The Arithmetic of Dynamical Systems. Springer. DOI: 10.1007/978-0-387-69904-2.

[21] Lapidus, M. L. (2001). Dynamical, Spectral, and Arithmetic Zeta Functions. American Mathematical Society.

[22] Mueller, J. and Shahidi, F. (2021). The Genesis of the Langlands Program (London Mathematical Society Lecture Note Series, Series Number 467). Cambridge University Press. DOI:10.1017/9781108591218.

 | DOI: 10.20533/jitst.2046.3723.2024.0107