

THE SAFE CAMPUS

USING PREDICTIVE ANALYTICS
TO ADDRESS SCHOOL SAFETY

CREATING SAFE CAMPUSES
FOR STUDENTS

BLUE LIGHT
PROBLEM SOLVED

This document includes data that is trademarked and proprietary to Blue Light LLC and can only be used with permission of Blue Light.

The content within is for informational consumption only and reflects the opinion of the company and its products. This paper cannot be considered as a proposal or basis for any contract or business relationship without contacting the company.

INTRODUCTION

Blue Light, a leading provider of predictive analytic solutions to industry, law enforcement, and the military, and its school violence prevention project, The Safe Campus, are honored to outline this concept detailing the critical need to deploy proven analytical solutions to address the critical issue of violence in American schools.

With over 14 years of experience and expertise in creating innovative solutions to address counter-threat financing, anti-terrorism, asymmetrical warfare, fraud, and criminal activity, the author feels that the issue of school violence could be more successfully countered if technologies, platforms and analytics proven to predict behavior or acts were to be used.

ABSTRACT

Most solutions focused on school violence are focused on reflexive or responsive measures i.e. physical security, active shooter training, exercises, social media analysis.

While these measures are critical, they are only beneficial when a violent event is pending or ongoing. To date, there have been minimal attempts to leverage the vast stores of data and information available from school systems, law enforcement, open source, social media and dark web data to conduct predictive analytics to mitigate school violence.

The use of predictive analytics applied to existing data sources can assist in the identification and intervention of violence before it happens.

PROBLEM

School violence is one of the most pressing issues facing the American educational system today.

The lethal nature of these attacks, combined with the continued inability to determine the actors or the methods of attack to be employed heighten the public's pressure on school systems, law enforcement and emergency responders to improve and if possible deter these attacks.

DISCUSSION

CURRENT SITUATION

School violence remains at the forefront of priorities for law enforcement, the educational system and parents due to its impact on society, families and innocent citizens.ⁱ

Attempts by schools to address school violence have increased but are largely confined to briefings, threat assessments, presentations, and training seminars until after 2015 when technologies such as social media, and anonymous texting platforms started to make their appearance. While a critical concern, school violence remains random in nature and largely unpredictable, hence the authorities' inability to get ahead of it.

Addressing school violence continues to be reactive measure, largely relying on physical security approaches and planning versus technical methodologies and analytics applications.

Technologies such as data analytics, social media analytics and integration of critical data sets – like school, hospital and law enforcement data – are very limited, if used, to address the possibility of predicting school attacks.

OVERVIEW OF SCHOOL VIOLENCE ISSUES

SCHOOL VIOLENCE CAUSES

There has been significant discussion regarding the cause of school violence in America. Blame has been made on everything; from the lack of 2-parent families to the use of social media, increase in bullying and economic uncertainty. ⁱⁱ

The range of backgrounds and supposed causes of school violence indicate that there is minimal common ground concerning the cause of violence on American campuses.

SCHOOL VIOLENCE TYPES

Besides the most devastating form of school violence, school shootings, violence on educational campuses takes many and varied forms from targeted violence by students, parents or caregivers, rampage violence or domestic terror. ⁱⁱⁱ

Despite the numerous forms of violence, there is one, bullying, that seems to be the most common denominator in extreme school violence, i.e. school shootings. ^{iv}

RESPONSIVE

Most law enforcement and school districts historically tend to address school violence with the perception of responding to an attack to minimized damage. These approaches tend to focus on "active shooter" scenarios, lockdowns (usually done simultaneously) and training law enforcement in the techniques, tactics, and procedures (TTPs) to intervene and remove active shooters on campus.

Other programs focused on physical security and relied on security audits to identify gaps in physical security measures and make recommendations to mitigate them. Hence, the significant increase in certain aspects of school physical security to include metal detectors, electronic locks, surveillance cameras, and other physical and

technical means. While an important aspect of school security and critical to limiting the access and/or range of an active shooter, these aspects have minimal value in the prediction and intervention of school violence. As a matter of fact, most papers released on school violence by FEI^v, FWG^{vi}, the Constitutional Rights Foundation^{vii} and even the Secret Service^{viii} still focus on responsive, physical methods and planning through threat assessments and exercises and not the inclusion of technology to get ahead of violent events.

INSTITUTIONAL COORDINATION

There has also been a marked improvement in the coordination and planning between school administrations and law enforcement.

Due to the societal impacts of school violence, the perception that these acts are a law enforcement problem and not the school's has changed to a point where schools are much more actively involved in the planning for violent attacks.

The coordination between law enforcement, the entire public sector – to include hospitals, transportation, fire etc. – is critical to ensure the myriad of issues related to these events are addressed. Communications, student movements, incident response, medical treatment, counseling etc., are all instances occurring during a violent event. Regular exercise drills with local law enforcement, planning techniques, improved communications etc. are designed to better identify and respond to school violence attacks.

INCREASED USE OF TECHNOLOGY

There has also been an increased acceptance of technologies to assist school authorities in addressing school violence. Recent programs train faculty and students to recognize some of the indicators of school violence, leveraging the use of social media analysis and texting platforms, to better identify problem students or persons that have been integrated into school violence planning to some degree.

Allowing schools to be more proactive in identifying individuals, reach out and intervene prior to a violent act being carried out

These are critical steps in the right direction implementing existing means of communication, taking advantage of the students' affinity for technology to collect vital data on potential school violence.

This is a game changer – going from a reactive approach based on enhanced physical and technical security to one based more on technology will be critical in being able to collect the information adequate to better predict events.

IMPACT OF THESE CHANGES

These and other solutions that have been applied to school security have undoubtedly prevented at least some attacks as they do limit key factors

- Open access
- Limited or no sensors, recording devices, or emergency devices
- The inability to recognize and report potential violent persons.

This success cannot be overlooked and the continued improvement of physical, personnel and technical security must be a fundamental base of any approach to school violence.

WHAT'S IMPACTING SOLUTIONS

LACK OF INTEGRATIONS/FUNDS

While efforts to address and prevent school violence have become numerous, the minimal integration of data, technologies and security improvements necessary to support these efforts, is still an issue. Most improvements in school security are individual programs disconnected/not integrated with past and/or future endeavors, reducing their effectiveness. Many, if not all schools, do not implement a scalable plan, aimed to have all efforts work in concert with each other.

School districts with limited funds or budget may encounter additional challenges in acquiring new technologies. Manpower-based solutions can be financially overwhelming.

IMPACT ON INFORMATION TECHNOLOGY (IT) ARCHITECTURE

Schools are cautious about any impact on their IT architecture. Given the sensitivity of data, the numerous data security, compliances (PCI, HIPAA, FERPA etc.), and the complexity of multi-tenant school systems, there's an unwillingness to implement solutions requiring extensive data manipulations (such as single data base storage or moving from a physical location to a cloud-based IT architecture).

CUSTOMIZATION

Many educational institutions have been exposed to shameless contracts and highly customized technological solutions holding them in servitude to the vendor for years. As solutions should be required to integrate with existing security measures, schools rarely opt for third parties customizations.

SENSITIVITY OF DATA AND PRIVACY

Due to its personal nature, school data is usually classified as Personally Identifiable Information (PII) or Personal Healthcare Information (PHI) and comes with onerous regulations under the HIPAA and FERPA acts, or oversight by privacy groups who feel the information should remain private.

Schools are reluctant to look at solutions not in compliance with the law, or that could expose information publicly when interfacing with their data.

CHANGING APPROACH TO SCHOOL SAFETY

The impact of school violence on our modern society has been all-encompassing.

While previously the impact was mostly felt in the affected community, recent school attacks have caused responses, and emotional devastation from everywhere around the U.S. (and the world), affecting how schools are safeguarding safety. For years, solutions such as armed guards, metal detectors, social media monitoring, student searches, expulsion, and so on were considered too severe or deprivation of privacy and student rights. However, today these and other approaches are being supported by greater numbers of parents, students, and teachers.

The recent national reaction to the Lakeland Park event shows concern from every level of society, and the willingness to discuss and introduce more stringent and responsive approaches. Schools are also adopting background checks on employees, hiring School Resource Officers (SROs) to assist with monitoring students, while other schools have on-duty police patrols in parking lots.

WHY PREDICTIVE ANALYTICS CAN HELP

The changes in school perspective have resulted in a demand for solutions that can more effectively address and prevent school violence.

Technical solutions leveraging existing school assets, making them an asset towards increased security and safety, are becoming more attractive and desirable.

UNTAPPED DATA SOURCES

The key to all predictive solutions is **data**.

Schools, their local environments, the internet are full of data potentially related to violent acts. To date, hardly any solutions are leveraging the vast stores of relevant on-site data, integrating them with other data sources to conduct predictive analytics. Becoming "predictive" entails for this data to be integrated and used in a proven, non-invasive manner to protect our students and loved ones.

Since the 1990's schools have spent billions of dollars integrating and updating technology. Estimates are the education technology market size is around \$8B per year.^{ix} While a large portion of this budget is invested in improving the use of technology and learning, it has also been used to digitize most of the data used by schools, including:

- Administration data
- Student data
- Teacher/employee data
- Counseling data
- Website and social media data

All these data sources are maintained by schools and available to be analyzed. Additionally, vast amounts of data relevant to violent events is available on the internet, social media, and the dark web, not to mention in public databases such as law enforcement and healthcare.

WARNING SIGNS

Recent reports indicate most shootings had some form of warning prior to the event.^x These warnings range from telling friends, to social media posts, to arrests, or mental health care treatment. These data touch points have become increasingly important in the drive to become more predictive in our approach.

PREDICTIVE ANALYTICS: A PROVEN METHODOLOGY

Predictive analytics, as a methodology, has had a significant impact on information analysis for decades. Making their appearance as early as the 1940s when Monte Carlo calculations first were used by the U.S. Government.^{xi}

What has become evident through the years is predictive analytics remain amongst the most sought areas of expertise in the market because of the increasingly complex algorithms, tools for insight, and ability to mine data. Every organization wants to know, as best possible, what the future holds. Predictive analytics is a proven means to determine that.

Since 9/11 there has been a rapid increase in the integration of tools and technologies into the predictive analytic environment. While information analysis was usually limited to papers, charts, diagrams, and other more conventional products, now it includes social media, cell phone activity, identity extraction, data searching and mining, web crawling, and even video analytics databases – resources not commonly used in the past, at least by military and law enforcement.

Predictive analytics are becoming more effective as the result of the vast available amount of new data to be analyzed resulting in solutions to identify and resolve not only violence-related issues like criminal activity and counter-insurgency, but also data driven-problems as insurance, healthcare, retail fraud, and cybersecurity.

AN OVERVIEW OF THE PREDICTIVE ANALYTICS MODULE

To the untrained eye, predictive analytics works as:

- A cycle of flowing information, data an analyst leverages to identify problematic individuals, entities, situations;
- Validating its accuracy to determine which entities reflect an actual threat
- Working with established authorities and rules to create mitigation strategies.

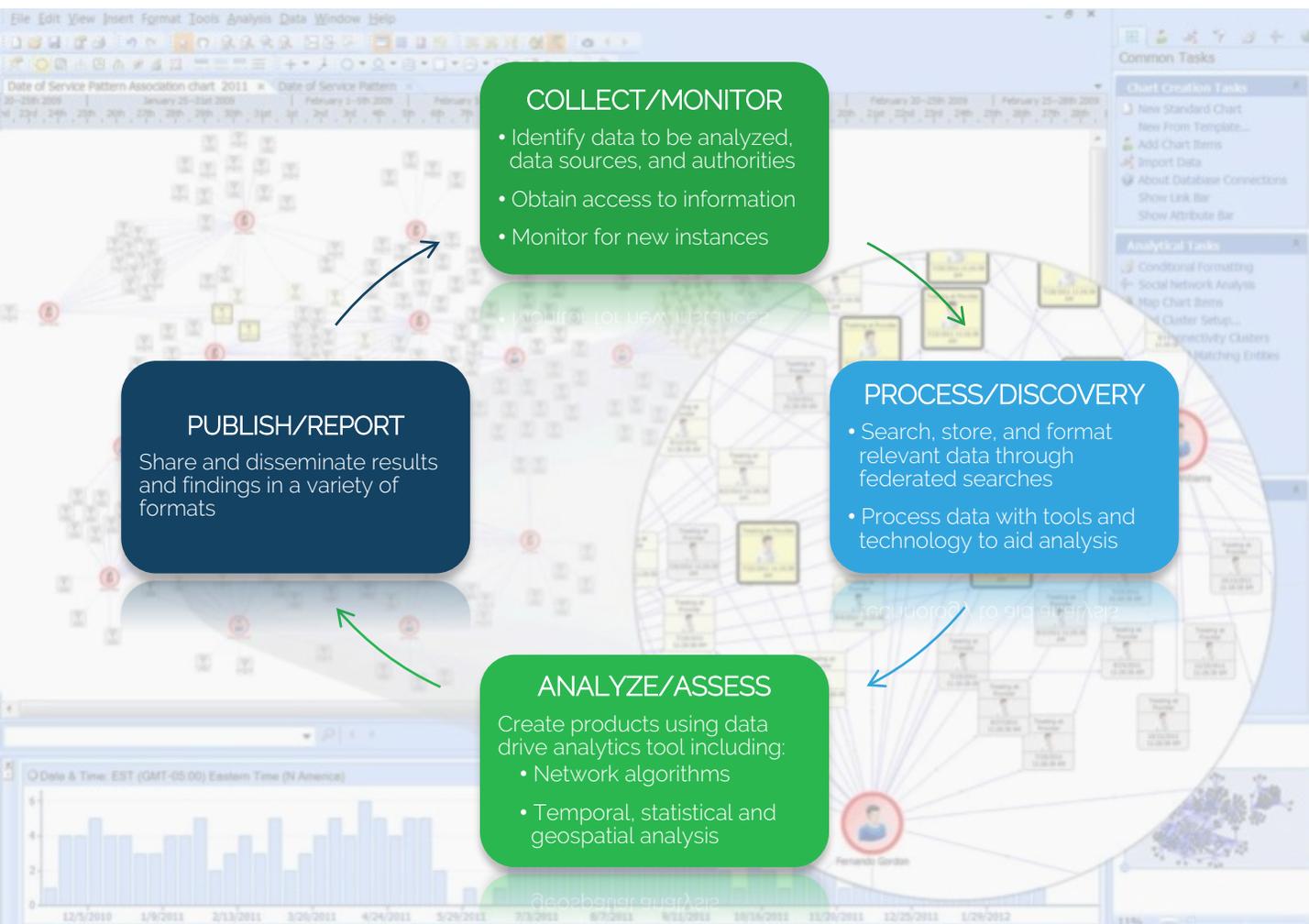
Depending on the scenario, the types of data, tools, and collection methodologies used may differ slightly, but the process remains virtually the same for any violence-related use case.

The **intelligence cycle** is the foundation of any predictive analytics models. It has been around for decades and has seen some shifts in its application such as the F3EAD (Find, Fix, Finish, Exploit, Assess, Disseminate) model used by Special Operations. The model in this document is based on this analytical foundation.

The goal of the of the intelligence cycle's analysis is to achieve an end-state aimed to form a decision in support of the analyst's findings. Once the decision is made, a new cycle begins to support a new event. There is no continuous monitoring of data to follow (.e. battle won, or case closed).

Our position in the case of predicting violent behavior involves a continuous process data analysis to identify potential patterns or anomalies leading to the identification of a potential offender and intervene as required or if necessary. In this model, the analyst would conduct the continuous monitoring of the originating and additional data sources, to quickly ascertain when an individual or a newly discovered entity may be prepared to act out. Once identified a decision and subsequent action would be required next. The analyst would continue to monitor the data sources for additional information relevant to the case.

PREDICTIVE ANALYTICS MODEL



Some variations of the intelligence cycle are present when applying predictive in targeting violent people. Following are the reasons:

- Predictive analytics relies on data. *"The more data the better"*, considering links and patterns become more evident when larger data sets are accessed/assessed. Data should be aggregated in such a way to allow future searches to be as easy as possible.

The end-user should identify as many relevant databases to school violence, i.e. internal records, law enforcement records (if possible), open source searches, chatroom searches, darknet searches and especially, social media.

- Predictive analytics data processing is more reliant on technology than conventional analytics. The data is processed, or translated, in a highly searchable data storage model, allowing not only for futures queries but also for time and resources conservation.
- The most successful models implement data connectors or ETL (Extract, Translate and Load) technologies to make data inter-relational, easy to query, and apply schemas and/or filters to organize it for predictive analysis.
- The recent proliferation of communication channels on the internet and easily identifiable sources of information have constituted a significant addition to the data sources available to analysts. Querying these sources daily, and when possible set up alerts to alert analysts of new and relevant information, is the key to true predictability. In this model, the analysis continues after reporting, monitoring relevant databases for future actionable information.
- Predictive analytics is an essential element of a solution platform, but not a solution in itself. Results are effectively produced when multiple data sources (vital records, sensors, cameras, internet, darknet, social media, etc.) are available, accessed, monitored, and reported on. While an organization may have access to several of these resources, it is indispensable to converge them on one platform to successfully identify potential events and initiate an appropriate response.

PREDICTIVE MODELING SYSTEM APPLICATION

It is critical to ensure the integration feasibility of the predictive analytics model into the existing school IT data and security plans. Any use of data or predictive analytics would follow a standard project management plan to satisfy requisites, including:

- **Data Analysis** – The vendor, stakeholders, school officials, security team, law enforcement, and other parties involved will assess the school's data sources, data architecture, and establish any system specific requirements to be implemented.

- **Database Connector(s) Identification** – Any required connectors for the database, open source, social media platform, and texting apps will be identified at this stage of the process.
- **Platform Delivery and Installation** – The system will be installed and configured according to an agreed upon timeline and in compliance with all school and federally mandated requirements.
- **Training** – The analysts(s), SROs, and/or other individuals involved in the project will be trained on the system.
- **Support** – The system will be handed over to the school as their property and maintained or sustained according to the contract.

Configurations of predictive analytic systems for schools can vary from a single system used by an SRO or Law Enforcement analyst, to an incident response center, to larger intelligence and response centers. The technologies used in conducting these types of assessments allow systems to be remote, and not physically at the school. Affording the possibility of merging additional schools in a single district. Depending on school requirements and/or budget, individual systems can be tied into incident response or command centers, where during an event, local assets such as police, fire, and medical resources can be involved.

Relations with local authorities, internal police forces, medical networks are another relevant factor in the configuration process. Collaborative relationships will ensure critical data (such as arrest records, health care issues related to violence) related to a potentially violent individual will be shared by these entities.

AN APPLICATION EXAMPLE

This example illustrates how a school would apply a Predictive Analysis model based on the one detailed above. We will refer to the Parkland school shooting as an example.

Blue Light was brought on to advise local Law Enforcement after the event. *(Any information related to the shooting comes from open source documentations)*

PLANNING AND DIRECTION

This phase provides the school administration and assigned staff the priorities for conducting predictive analytics with sensitive data. During this process, the authorities determine what threats are oriented towards the school based on historical data (i.e. bully, bomb threats, harassment, shootings etc.), and prioritize them for the analyst. Consideration of data sources is also critical in creating the largest possible repository for analysis. Depending on the scope, schools should be looking at their own data, regardless of the type or form, and any other sources they would like to query, i.e. law enforcement, open source, dark web data etc. Attention should be placed on any limitations or compliance requirements to ensure the data is accessed in accordance to the law/regulations.

In the Parkland shooting case there were several data sources that, if available to an analyst, would have provided information regarding the shooter. He had records and reports in the school, law enforcement, local medical systems, as well as social media.

COLLECTION/MONITOR

Identify data to be analyzed, data sources, and authorities | Obtain access to information | Monitor for new instances

During this phase, the analyst is querying the approved databases, texting platforms, social media alerts as well as law enforcement, state and federal databases, if possible, for relevant information. The information would be stored in an onsite database behind a firewall for processing and subsequent reporting. If information identifying an immediate threat is found, the school should escalate it to the attention of the authorities.

It is quite possible the Parkland shooter might have been located as data relevant to him from school, law enforcement, and social media records would have been processed during this phase for analysis and assessment. Monitoring of the data would have brought new information regarding arrests or social media posts into the analysis flow.

PROCESS/DISCOVERY

Search, store, and format relevant data through federated searches
Process data with tools and technology to aid analysis

During this phase the school analyst takes the data from the earlier queries, applies it to an existing or new use case, and readies it for analysis by applying filters, algorithms, and schema to make the data inter-relational. Data determined to be irrelevant is dumped, while data driving other cases may be discovered, and initiate new cases begin based upon it.

Any information collected is formatted in a way to simplify the association between a potentially violent person to events and actions that would become increasingly evident in the next phase.

COLLECTION/MONITOR

Identify data to be analyzed, data sources, and authorities | Obtain access to information | Monitor for new instances

At this point the school analyst is applying more advanced tools and technologies to analyze the data in order to identify links between entities and events, update existing cases, or linking a potentially violent offender to an immediate threat. Analysis is continuous, on a daily basis new data is being analyzed to value its connections to existing use cases. Threats identified are validated through data sharing or vetting with authorities prior to submission as a report.

This would have been the step in the process where the Parkland shooter could have been identified. The data collected by no would have been difficult to overlook. Using link and temporal analyses, and identity extraction tools an analyst would be able to identify numerous events that would indicate intervention is needed.

PUBLISH/REPORT

Share and disseminate results and findings in a variety of formats

In this final phase the analyst prepares the report to submit to the authorities for validation and action. The report can be produced in any required format but should contain the information necessary to support the analyst's claim. If required, supporting documentation can be provided from the use case assigned to the individual.

PREDICTIVE ANALYTICS' KEY FEATURES

A review of technical systems employed to provide predictive analytics for use cases outside of school violence, identifies key features that would add value to a school violence prevention platform based on predictive analytics. They are:

AFFORDABILITY/BUDGET AWARE

In light of the budgetary woes affecting numerous school districts, as well as parents, it is critical that any solution should have minimal impact on a school budget, not only in the original monetary outlay required to acquire for it, but also over time. Predictive analytics solutions take this into account.

Getting approval for the purchase of a predictive analytics system will have to be worked on and innovative approaches to funding may be needed. In most major cities there are business supported non-profits offering funds to be used for projects like school violence prevention. Grants are also available and a bill is currently going through the United States Senate, called the STOP School Violence Act, that will provide \$1.2B in funding accessible for purchases.

PROVEN

Predictive analytics platforms are solutions can be utilized for decades, with regular updates on technologies, training, and technical support. Reliance on "out of the box" solutions, as opposed to customized ones, is also key as it provides school districts the flexibility to receive support from several sources.

TECHNOLOGY-BASED

A predictive analytics platform is a solution based on current technology, able to integrate a myriad of data sources.

SCALABILITY

One of the many advantages of predictive analytic is scalability – the platform will scale to the size of the dataset or use case been applied to. The ability to scale to the growth of a school district, or vast increases in data available, to better conduct analysis is key for success.

INTEGRATION-READY

Predictive analytics solutions are “IT-friendly”, easy to customize.

COMPLIANT

Our solution is HIPPA and FERPA compliant.

CONCLUSION

- School violence is the most pressing concern facing schools and parents across the country today.
- A comprehensive, analytical approach is required to take schools from a reactive mode to a predictive one.
- It is critical existing data on the internet, social media, and within schools is aggregated and analyzed to identify any potential violent offenders as early as possible with the intent of intervening before a situation escalates.
- Predictive Analytics are one of the few solutions able to harvest all the data available to schools ensuring a more comprehensive scenario of the school's population and any threats against them is formed.
- Schools and law enforcement authorities can make informed decisions relevant to the threats and can be more effective in halting the unfortunate issue of school violence.

ABOUT THE AUTHOR



Bruce Parkman is the CEO of Blue Light LLC, a premier provider of data analytics solutions addressing some of today's toughest law enforcement, military, and commercial challenges.

Bruce is the founder of The Safe Campus, a project that uses the methodologies here to address school violence issues.

Learn more at BlueLightLLC.com and TheSafeCampus.com

REFERENCES

- i. <https://everytownresearch.org/gunfire-in-school/#>
- ii. <https://teens.lovetoknow.com/cause-effect-school-violence>
- iii. Buerger, M.E., Levin, B.H., and Schafer, J.A.(2018). Examining school violence: A consideration of select future avenues. Futures Working Group, Society of Police Futurists International.
- iv. <https://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf>
- v. https://www.feinet.com/sites/default/files/news/attachments/School%20Violence%20Prevention_FEI_2012_0.pdf
- vi. Buerger, M.E., Levin, B.H., and Schafer, J.A.(2018). Examining school violence: A consideration of select future avenues. Futures Working Group, Society of Police Futurists International.
- vii. <http://www.crf-usa.org/school-violence/school-violence-prevention-strategy.html>
- viii. https://www.secretservice.gov/data/protection/ntac/USSS_NTAC_Enhancing_School_Safety_Guide_7.11.18.pdf
- ix. <https://www.edweek.org/ew/issues/technology-in-education/index.html>
- x. <https://www.wusag.com/article/news/local/next/a-look-at-every-school-shooting-andthe-warnings-signs-before-they-happened/73-531119651>
- xi. <http://www.fico.com/en/latest-thinking/infographic/the-analytics-big-bang>

BLUE LIGHT

P R O B L E M S O L V E D