A Framework for Cyber Incident Modeling

June 2012

Cameron DePuy

Brendan Farrar-Foley

Rachael Greenspan

John Thompson

Bert Watson

Table of Contents

This paper was completed with generous guidance from Dr. Greg Larsen, Dr. Margaret Myers and Ms. Laura Odell.

Section I: Introduction

Human interactions in, through, and from cyberspace are common in everyday life The analysis and understanding of individual known incidents has been documented and studied by many including those in the cyber field. The practice of completing a case study for a single incident explored in great detail is useful. However, a multi-faceted meta-analysis including examination of precursors to a specific event and ramifications (implicit or explicit) over time offer an overarching benefit. By observing the history of past conflicts and national security events, future generations are afforded the opportunity to understand susceptibilities and the consequences that may occur via multiple real life scenarios, and leverage that knowledge to make informed decisions for future strategies. One must be able to reference and correlate significant happenings over time and link incidents that are comprised of and result in changes of behaviors and capabilities. The intersection of these behaviors and capabilities can only be understood if there is a common framework in which incidents may be linked to explain the rapidly changing environment. Cyber incidents are no exception.

This paper proposes a framework for exploring cyberspace by examining historical incidents (case studies) in a common manner. In the context of this paper, a *cyber incident* is the observed intersection of human behavior and cyberspace capabilities. By providing a vehicle for examining historical incidents, the framework can be used to craft a *future history* of possible incidents and the boundaries around such possibilities. The framework assists in examining trends in behaviors and technologies that interact to provide benefits and the potential for malice, mischief, or error. The framework generates knowledge by exploring multiple historical incidents in cyberspace to facilitate contextual understanding of individual incidents and the implications for future incidents, whether the context remains unchanged or is altered.

The remainder of this paper is organized as follows. Section II provides background information on cyberspace, cyber incidents, behavior and capability interactions, and incident modeling methods. Section III describes the framework and shows how cyber incidents may be mapped over time and understood in a comprehensive, unprecedented form. Section IV discusses potential uses of the framework and future questions to be explored related to the framework.

Section II: Background

Cyberspace as Environment, Domains as Purposeful Cyber Operations

Environments are the *surround*; the commons. Cyberspace is an environment that is wholly constructed and not occurring naturally – although dependent on natural phenomena to be implemented. An environment can be partitioned into domains of operation(s). A social domain, a political domain, a business domain, a war-fighting domain, etc.; all partition the environment – in this case cyberspace. Humans can interact with natural environments without any machinery. Humans breathe air; they do not emit bits into an Ethernet cable. Thus humans require an aperture to enter, interact with, and exit from cyberspace – often loosely described as a *persona*. Humans only exist in cyberspace as mediated agents. As in any partitioning of a man-machine complex, humans and machinery combine to conduct operations with a specific purpose or intent. Those operations may be in support of some other environment or domain within another environment; or specifically to gain advantage within cyberspace for an operational purpose that only exists within cyberspace. Thus the idea of operations in, through, and from cyberspace arises.

Cyberspace is a constructed environment that is dependent on a unique relationship between humans and technology. Cyberspace is comprised of advancing technologies and virtual connectivity, but, "the complexity goes beyond that of natural systems because it also involves human strategic interactions."[1] Because of the reliance and focus on technology, it is easy to forget the importance of the human. Without human interaction, cyberspace would lose its purpose and its ability to evolve. Other military operating environments (i.e. land, sea, air, space) do not have the same dependence on humans for existence nor do they require a human-to-machine interaction. The Center for New American Security describes the cyber domain as "unique in that it is man-made, recent and subject to even more rapid technological changes than other domains."[2]

Other environments may be used to draw some analogies to the strategic dependence a user may have in cyberspace. Just as the sea environment is restricted to water-related engagements, cyber activities are typically limited to the networks and connections involved in a particular transaction. All activities may be bounded by limitations the environment presents. However, the bounds for the cyber environment are constantly changing due to rapid technology change and social hyper-connectivity enabled by mobile and network technologies.

Incidents occur often in the cyber domain because of these constantly changing factors and the lack of governance and authority over the domain. As with the other domains, the cyber domain is global and difficult for one group to control. A single packet routing activity can cross

[1] Lord, Kristin and Travis Sharp. "America's Cyber Future, Security and Prosperity in the Information Age". Center for a New American Security. Volume 2. June 2011.

[2] Lord, Kristin and Travis Sharp. "America's Cyber Future, Security and Prosperity in the Information Age". Center for a New American Security. Volume 2. June 2011. Pg. 9

into several different countries and several different layers of ownership and responsibility. Is the country in which the data originates responsible for safe delivery? Or is it the service provider? Or is it the routing device manufacturer? The author? The government? Which government? Laws typically change at physical or political boundaries; barriers not easily migrated to the cyber environment.

There are also several challenges in costing and understanding the impact of incidents in the cyber domain. A recent study by the Security and Defence Agenda, a NATO dedicated security and defense think tank, points out that, "It has taken the spectacular increase in cyber-attacks for political leaders in the United States, the European Union and parts of Asia to sit up and take stock of the costs involved and the loss in competitive positions"[3]. There is no good mechanism for understanding and tracking incidents that are occurring in the present, or a consistent model for predicting future events.

Cyber Incidents

Cyber incidents are of much more concern today than they were in the past. The first known cyber incident was the Morris Worm in 1988[4], which was the first widespread worm distributed across the Internet. For this reason it was the first cyber attack to garner significant mainstream media attention and it resulted in the first conviction under the US Computer Fraud and Abuse Act. It should be noted that, the attack was successful partially due to weak passwords; still one of the most common cybersecurity issues today. The incident prompted the funding of the US Computer Emergency Readiness Team (CERT) at Carnegie Mellon University

[3] Grauman, Brigid. "Cyber-Security: The vexed question of global rules". Security and Defence Agenda Report. February 2012. Pg. 22

[4] http://en.wikipedia.org/wiki/Morris_worm

to provide a central place for coordinating responses to future cyber incidents. The estimated damages attributed to the Morris Worm was between $100,000 and $10,000,000 dollars, a relatively small sum today given the percentage of the Internet it affected[5].

Cyber attacks today have the potential to be far more devastating. Potential problems include degradation, manipulation, and loss of data and information available via electronic means. A cyber incident has been defined several ways depending on the point of view, perception, or interest of the observer. The Defense Industrial Base (DIB) Information Sharing Program has defined a cyber incident as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein."[6] This definition is limited to computer networks and the information within. It does not consider the points where cyber and physical environments interact.

The Center for a New American Security defines a cyber incident as "a cyber attack, exploit or intrusion that causes harm to critical systems, assets, information or functions across the public and private sectors by impairing the confidentiality, integrity, or availability of computers, electronic information and/or digital networks."[7] This definition takes an information assurance approach and does not address the potential for a cyber-physical impact.

[5] United States General Accounting Office. "Virus Highlights Need for Improved Internet Management". Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives. June 12, 1989.

[6] Department of Defense- Defense Industrial base Voluntary Cyber Security and Information Assurance Activities. Interim Final Rule. http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf. April 30, 2012. Pg 4

[7] Lord, Kristin and Travis Sharp. "America's Cyber Future, Security and Prosperity in the Information Age". Center for a New American Security. Volume 1. June 2011. Pg. 12

A cyber incident may have a physical impact and may occur by using information and communication technology (ICT) components unrelated to computer or digital networks. A successful cyber attack has the potential to cripple a city or destroy critical infrastructure. Supervisory Control and Data Acquisition (SCADA) systems are accessible via networks that can now be reached from the Internet. Often the controls for these physical systems can be modified in ways that remove the coded limitations on the operations of the physical equipment.

In the same way that cars have a computer limited maximum speed, most industrial systems have software-controlled aspects that limit the ability for damage to occur to the equipment. For equipment such as power transformers or sewage control systems, the repercussions of a cyber attack can cripple the equipment to the point that it is too damaged and must be replaced. Ordering, procuring, and installing new equipment can take months or years while a cyber attack can happen almost instantly.

One of the main challenges associated with defining cyber incidents relates to the inconsistent lexicon and partitioning of the characteristics that make up an incident. Appendix A provides an initial attempt to define the attributes of a cyber incident. Although this work is not the focus for this paper, it provides insight into the complexity of a cyber incident and leaves room for future work and exploration.

This paper proposes that cyber incident may be described as the intersection of a set of behaviors demonstrated and a set of capabilities available at the time of the incident. Behaviors

and capabilities may be used to describe the environment before, during, and after a cyber incident.

Behavior and Capability Changes

Cyber incidents may be described as the intersection of a set of behaviors demonstrated and a set of capabilities available at the time of the incident. Behaviors and capabilities may be used to describe the environment before, during, and after a cyber incident. Behavior is defined as the way in which a person acts in response to a particular situation or stimulus. Behavior change may be difficult to measure but it can be observable over time by aggregating policies, public impressions and incentives. A capability is defined as having the capacity to be used, treated, or developed for a specific purpose[8]. Cyber capability changes may be tracked over time by observing the evolution of technology and the proficiency in using the technology. These two variables describe the physical enablers of a cyber incident at a point in time, a set of behaviors (the current feelings and attitudes of society surrounding an incident at that same point in time), and a set of capabilities.

It is important that those working in the cyber field have a basic understanding of past events, are observant of what is occurring at present, and are constantly anticipating what is possible in the future. To become proficient in any field, one must be able to reference and correlate significant happenings over time and link incidents that are comprised of and result in changes of behaviors and capabilities The intersection of these behaviors and capabilities can only be understood if there is a common framework in which all incidents may be linked to explain the rapidly changing environment.

[8] http://www.thefreedictionary.com/capability

Although both behaviors and capabilities may be seen as independent variables, the cyber domain presents opportunities for interaction. This interaction may be deliberate or happenstance. For example, a major shift in US policy, the 401(k) provision, was created in 1978 as part of that year's Tax Revenue Act, affording every working American the opportunity to create tax-deferred retirement income. The policy change drove financial institutions to invest in and enable an automated technological capability demanded by investors who wanted to monitor their plan, first telephonically, and then over the Internet and to make real time changes in their investments. This led to further behavioral change where the capability created a human expectation of hyper-connectedness; to immediately know the status of funds and transactions. In this case, there was a direct connection between behaviors and capabilities. The political domain drove a change in behavior and the changes to behavior incentivized the use of automated technology.

Whether the interactions between behaviors and capabilities are planned, the impacts of those interactions may be consistently measured by four parameters and the impact of a cyber incident may change according to the point of view of the affected parties. The impact may be:

1) Beneficial or with consequence,
2) Large or small,
3) Relevant or non-relevant,
4) Significant (long term) or insignificant (short term)

These parameters may be used to gauge the level of interaction at a point in time and to compare incidents. Dividing incidents into the intersection of behaviors and capabilities and

scaling the impact level by four parameters leads to a consistent modeling framework for cyber incidents.

Incident Modeling Methods

The practice of completing a case study for a single incident explored in great detail is useful. This analysis and understanding of individual known incidents has been documented and studied by many, including those in the cyber field. However, a multi-faceted view including examination of precursors to a specific event and ramifications (implicit or explicit) after the event offers a more overarching benefit. By observing the history of past conflicts and national security events, future generations are afforded the opportunity to understand vulnerabilities, via multiple real life scenarios, and to leverage that knowledge to make informed decisions for future strategies.

A survey of field of work reveals four main methods of incident modeling used for cyber incidents.

- Via targeted observation.
- Through voluntary information sharing.
- Through historical trending.
- Based on an ad hoc discover and respond construct.

Although some overlap between the methods exists, all of these methods lack a standard lexicon and consistent way to observe multiple events in a shared environment.

Targeted observation is discussed in a McAfee White Paper on Operation Shady Rat. Operation Shady Rat was an investigation into targeted intrusion into 71 organizations over five

years.[9] These incidents were all carried out by the same threat actor but targeted a variety of victims. For all incidents, the method of attack was spear-phishing via email. Because of these similarities, it is possible to collect data and draw conclusions to prevent a similar attack or identify where it may have originated. Lacking is the ability to relate these incidents using the documented data to incidents that do not meet the targeted parameters. The focus for the comparison and analysis of events is limited to the targeted nature of the incidents.

Voluntary information sharing is important in discovering, recovering from, and possibly preventing previously experienced or forecasted cyber incidents. However, the voluntary nature has made it difficult to collect consistent data since a common lexicon is not used to compare multiple incidents.

For example, the Defense Industrial Base and the US Government participate in a voluntary information-sharing pilot for cyber incidents. The pilots provide a way for the community to learn about certain attacks and to possibly prevent them from continuing in the future. Each incident report is assessed individually and the reports are dependent on how much information was actually provided. The information sharing is limited to known incidents and has a limited definition of what triggers a cyber incident and should be reported. Although data has been collected on these incidents, no framework exists to normalize the data to make it comparable to other incidents or outside this small pilot.

Another voluntary information sharing effort called the Index of Cyber Security (ICS) was established in 2011 and is being led by Dr. Dan Greer and Mukul Pareek. The ICS has created a mechanism for tracking cyber incidents by aggregating views of information security

[9] Alperovitch, Dmitri. “Revealed: Operation Shady RAT”. McAfee Threat Research. 2011

professionals through a monthly survey. The monthly survey asks about fifteen areas of cyber security issues and the participants rate each on a scale of: rising fast, rising, static, falling, or falling fast. The ICS is consistent in its questions because it wishes to establish an "ongoing, methodologically transparent measure of the state of cybersecurity." The ICS survey is unique in that it asks consistent questions, receives a defined range of responses and is collecting the data over time. More information on the Index for Cyber Security may be found in Appendix A.

Historical trending of cyber incidents is summarized in a paper by Shimeall and Williams on cyber incident trending methods and considerations. Topics such as the identifying factors of temporal, spatial, or associational cyber trends are discussed. Associated issues and difficulties with the search for these trends in cyber data are also summarily introduced. Baseline creation, incorrect inferences about causation, and dataset creation difficulties are all listed as illustrative examples of problems that hinder a cyber-trend analyst. The strongest part of the paper is the inclusion of several cyber-trend examples, complete with representative graphs that exhibit trending. While this paper is geared towards cyber trending at the system level, it takes on the topic with enough generality that many of the concepts are equally applicable in the macro-cyber sense. The approach is limited as a theoretical primer on the concept of cyber trend analysis, as it makes no attempt to be a technical or comprehensive guide.[10]

The fourth method of cyber incident modeling is retrospective, ad hoc evaluation. This means that there is no structured collection of data and no method for comparing incidents. Project Enlightenment is a case study that took place over six months on one cyber incident

[10] Shimeall, Tim, and Phil Williams. "Models of Information Security Trend Analysis." CERT Analysis Center, Software Engineering Institute. April 16, 2012 <http://202.41.82.144/data/HACKING_INFORMATION/PRINTED%20PAPERS/models%20for%20inf%20security%20TREND%20ANALYSIS.pdf>.

report that peaked interest for further observation. This one incident was determined to be one of many similar incidents being conducted by a single adversary. A team at Cyber Squared discovered this single adversary had collected data on the espionage campaign. The data collection on the incidents was ad hoc in the sense that as the research progressed, the team determined what they should record and what statistics they should collect for reporting purposes. Those affected did not know their systems had been compromised. The investigation conducted relied on discovery methods. Once more incidents were linked together through intelligence work, the proper response could be addressed. Uncovering the interplay between cyber incidents is important but the lack of structure and defined methods makes it difficult to scale to include all cyber incidents.

Section III: Framework

Current cyber history and future cyber history will only be understood if there is a common framework in which incidents may be linked to explain the rapidly changing environment. This framework is intended to set the stage for cyber forecasting by understanding how cyber related behavior and capability interactions have evolved over time. If capabilities and behavior interactions can be characterized, a common framework can be created for all cyber incidents to be mapped over time and viewed in a comprehensive, unprecedented form.

Cyber incidents have a broad and deep reach as man-machine interaction has produced information and communication technology (ICT) systems that are embedded in and control physical infrastructure that runs factories, cities, and countries. Resulting cyber incidents have the potential for much broader impact than ever before, culminating in a physical impact.

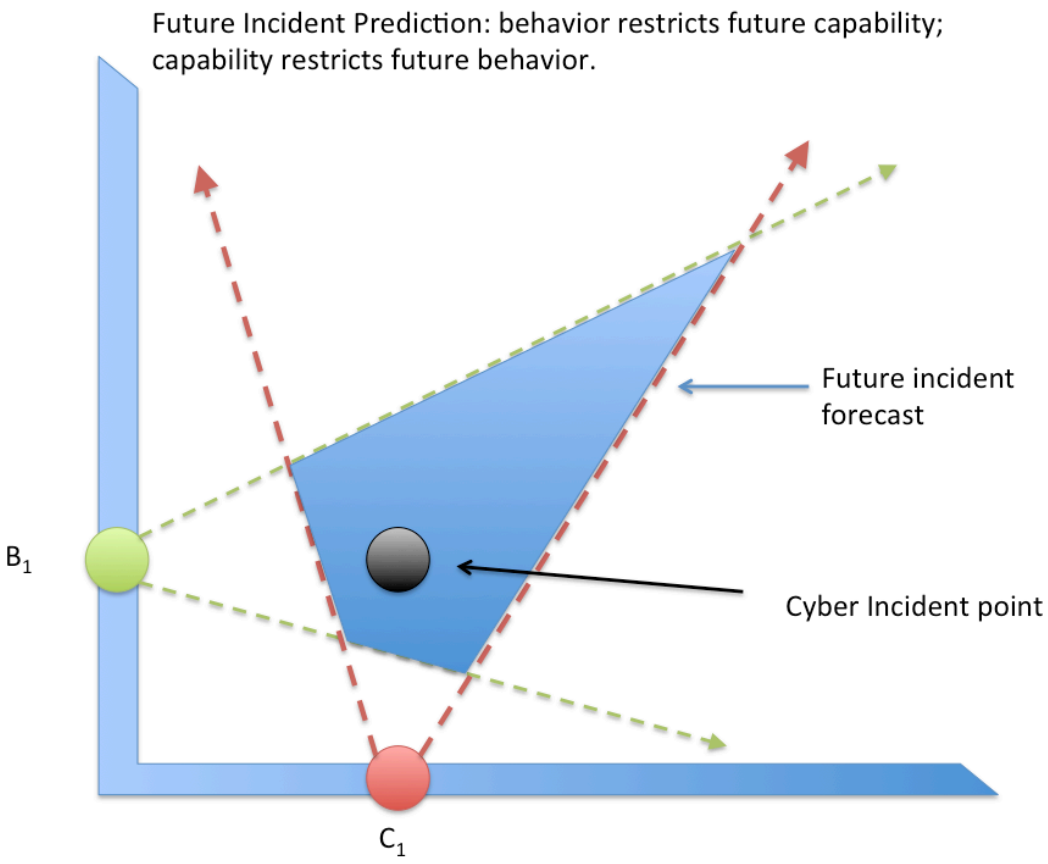

Figure 1

Caption: Shows the relationship between behavior and capability. A cyber incident is possible at the intersection of a set of behaviors (B_1) and capabilities (C_1). From each axis we can draw lines of likely future behavior or future capability. The intersection of these areas provides a "future incident forecast" where near future cyber incidents are likely to occur. From this one might predict the future behaviors and capabilities that may interact to produce a specific cyber event.

Behaviors encompass the human response and perspective. Behaviors include reactions to policies (laws, regulations, policies), interpretations of those policies, public impressions, and other human elements.

Capabilities encompass the technologies and know-how (ease of use) to utilize technologies to produce a result.

While behaviors and capabilities can be considered independent variables, cyberspace, and the other operating environments, presents opportunities for them to interact. These variables are dependent on one another in that current capability influences future behavior and current behavior impacts future capability. The interaction of behavior and capability can be deliberate or happenstance; (i.e., a specific policy may be introduced which limits the use or function of a particular technology).

Because behaviors and capabilities interact in cyberspace, they can be used to predict likely future cyber incidents by predicting the bounds of probable future behavior changes and the probable future capability developments. The intersection of the likely future behaviors and capabilities produces a future incident forecast in which future cyber events are likely to fall. If the range of future incidents can then be predicted, one can prepare for those specific events.

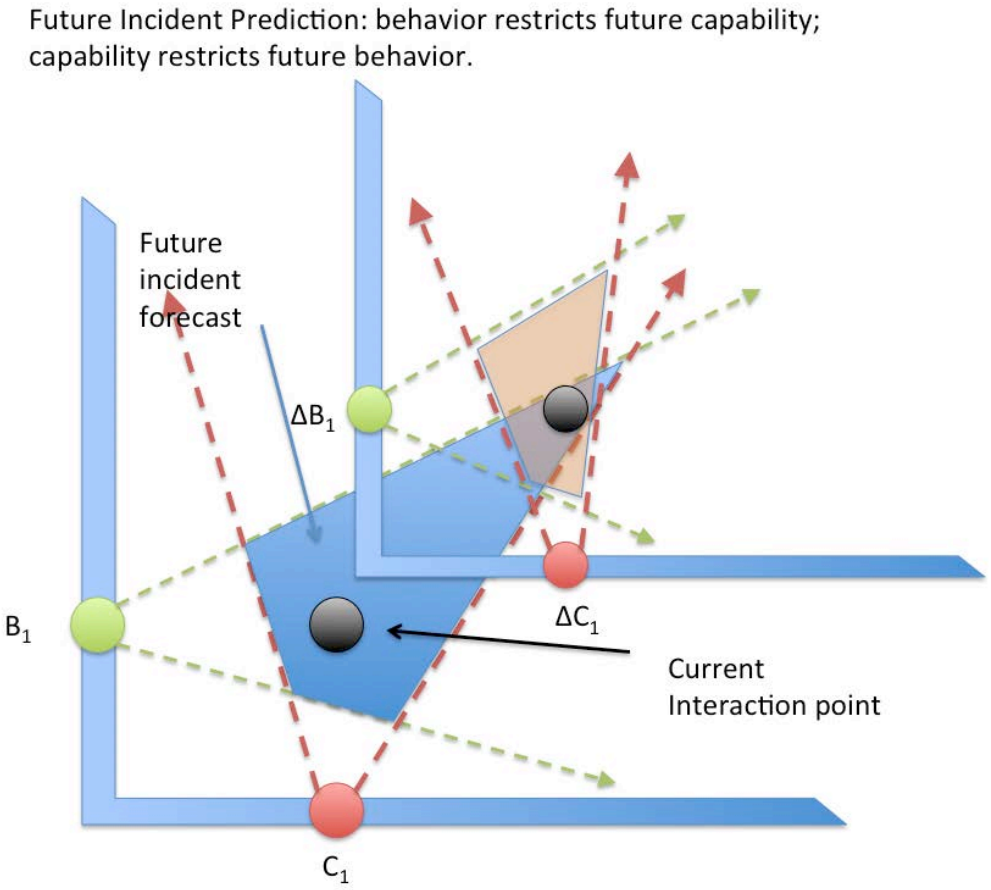

Figure 2

Caption: Leveraging the previous figure, this graphic shows the original future incident forecast as well as a secondary event. The secondary event falls within the original event's forecast area. At the point of this secondary cyber incident, new behavior and capability predictions are made yielding a new future incident forecast. Notice that future forecasts include potential for a reversion to earlier capability or behavior sets. Older technologies or behaviors may be re-enacted in an attempt to confuse or manipulate a victim using changed behaviors and capabilities.

This forecasting allows for prediction of future cyber events. Given this small subset of predicted (vs. total) potential events, behaviors can be changed and capabilities developed to shape the specific future incidents. The events are influenced by the incentives introduced to create certain behaviors or develop certain capabilities. Similarly, deterrents can reduce specific behaviors or discourage development or distribution of a capability. Careful adjustment of incentives and deterrents bound future events to a controllable set, greatly reducing risk from the environment.

Cyber Incident Cycle

Understanding the combinations of behaviors and capabilities will allow for situational agility and the ability to produce optimal future incident forecasts to reduce cyber risks to a tolerable level.

A set of behaviors and a set of capabilities present at some point in time have the potential to combine and form a cyber incident. In response to this incident, behaviors, capabilities, or a mix of both will change. The new sets of behaviors and capabilities form the potential for another cyber incident.

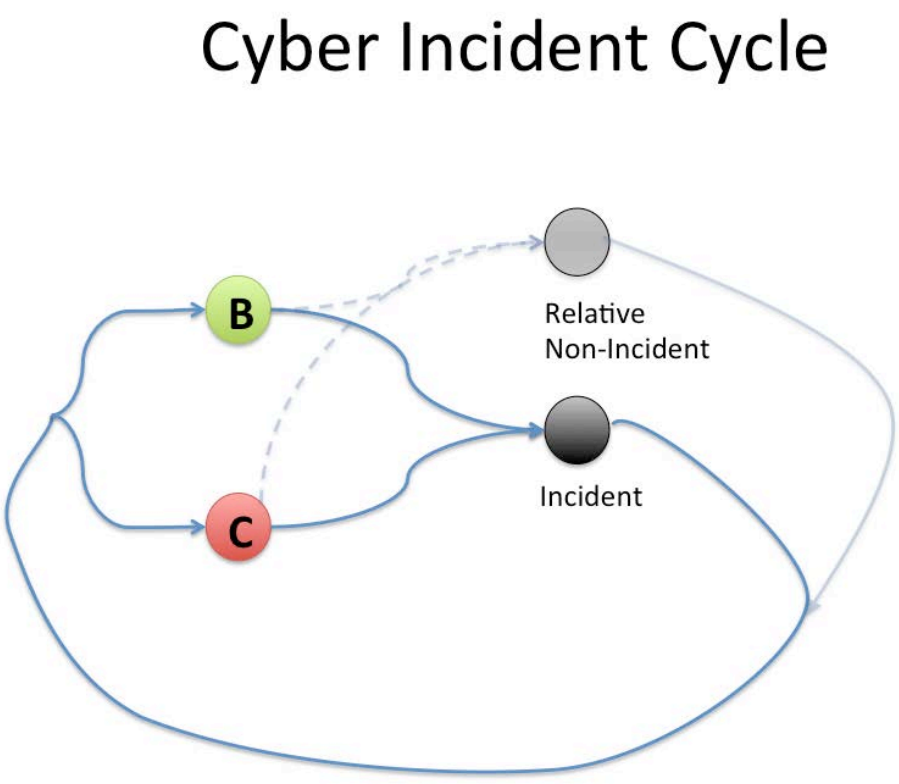

Figure 3

Caption: A cyber incident cycle exists where the current Behaviors and Capabilities combine to form a cyber incident. In response to this incident, changes are made to behaviors (e.g. policies) or capabilities (e.g. technologies). After these changes, the potential for a new cyber event exists. By enacting certain behaviors or capabilities *preemptively* we may avoid specific cyber incidents or transform a devastating incident into a relative non-incident. Those charged with protecting cyber infrastructure must constantly strive to change behavior and capability to produce non-incidents and avoid catastrophic incidents.

Forecasting Cyber Incidents

Planners in any domain continuously seek knowledge to forecast possibilities, put bounds on the possibilities, and provide a basis for informed decisions. To gain this knowledge and use it effectively requires an empirical framework in which observations (interactions of behavior and capability) can be measured, trended, and most importantly, acted upon to shape the consequences of an interaction.

Forecasting of future cyber events may allow for changes in behavior or capability (see below) to minimize unwanted consequences:

- Eliminate the possibility of that incident reoccurring (by changing behavior or capability to make it impossible).
- Substitute the incidents chance of reoccurrence with another incident.
- Increase or decrease the likelihood of specific incidents by attempting to influence behavior and capability outside of the objects included in the incident.

As a simple example, consider a rash of window breakings in a neighborhood. While a window is easily broken, the following steps can be taken to change this incident in the future:

- Elimination can occur by strengthening the windows to make breakage very difficult. This option largely solves the problem by increasing the capability of the windows but comes with disadvantages that include high cost.

- To substitute this incident for another, punishment for the crime of window breaking could be greatly increased thus making other petty crimes more attractive to would-be criminals. This provides a dis-incentive for a criminal to utilize his window smashing capability.
- To decrease the likelihood of this incident, police patrols could be increased. This changes the behavior of the protectors of the infrastructure (i.e. windows) in the hope of influencing the behavior of the attackers.

In this example, the availability of windows, the ease of breakage (capabilities), and the lack of dis-incentive for would-be criminals provide a likely incident of window breakage. By evaluating these factors before an incident occurs, measures such as those above can be taken in advance of the incident to create a non-incident (see figure 3) rather than reacting to a high rate of window smashing.

Evaluating current and past cyber incidents and making predictions on future behavior and capability (providing the future incident zone) indicate a potential range of future cyber incidents. The task of protecting cyber infrastructure (including adjacent physical infrastructure) must constantly evaluate these incidents and anticipate future incidents to provide preemptive capability and behavioral incentives designed to avoid cyber incidents above a tolerable risk level.

To preemptively take action and change behavior and capability, the interaction between capability and behavior must be understood. When building, implementing, or discovering a capability, the effect on future behaviors and future capabilities must be examined. When

considering behavior change (i.e., policy changes), an evaluation of the impact of those policy changes on future behavior and future capability must be undertaken.

Behaviors and capabilities can be influenced to produce known effects in the environment? To illustrate, consider a typical example of email attachments process and policy.

1. When an early email system is introduced, attachments are unregulated.
2. Shortly after email attachment capability exists, an adversary gains the capability of spreading viruses via email attachments.
3. In response, the company creates a policy that email attachments from unknown parties are not to be opened. At this point there exists no capability for the company to enforce this policy, or track its compliance. The company will continue to scan for viruses in hopes of finding and repairing any machine infected through email or other means.
4. At a later time, the company implements policies via installed software that prevents an attachment from opening unless the sender is in the local address book. With this comes the capability to monitor whether the policy is being complied with and prevents an incident before it occurs (proactive). This improves on the original practice of determining the policy had been broken when an incident occurred (reactive).
5. At a much later time, the software amasses data on additional user and malicious attachment behavior. The additional information afforded allows fine-tuning of future policies and behaviors to bring them inline with the enhanced capabilities now available. This is ideal as it not only preemptively constrains cyber incidents, but also opens additional possibilities for proactively discouraging types of future capabilities and incidents.

Behavior and Capability Interaction

To see the interaction of behaviors and capabilities and look at how they influence each other, we can examine the music industry in the 1990s. The industry experienced incidents as MP3 technology, a new capability in digital music, became available and then widely adopted. In this example, behaviors evidenced by the adoption of technologies while capabilities are the technologies themselves.

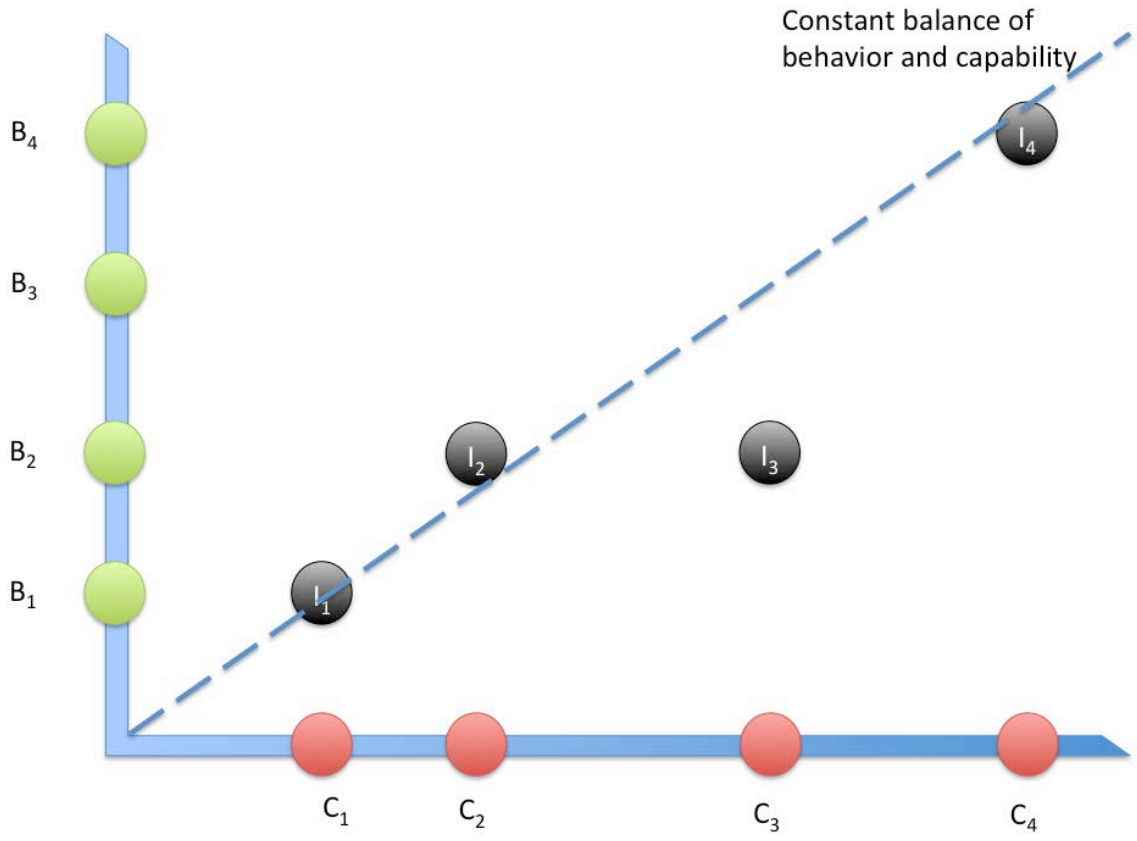

Figure 4

Incident point $I_1 = (C_1, B_1)$ = early 1990s. Music is available (in this example) as persistent media via CDs and as streaming media via radio stations. Notice that this incident falls on the line indicating a balance between behavior and capability; it is at equilibrium.

In the mid 1990s, MP3 technology becomes available (C_2). This technology allows for the storage and playback of digital copies of music on a desktop computer. With digital copies the quality of the music playback is very high, and the ability to make an additional copy and transfer it to another individual is trivial. Previously (i.e., cassette tapes) the playback quality was mediocre, and the ability to copy degraded the quality of the music each time a copy was made.

Soon after MP3 technology is available it begins early adopters begin using the new technology (B_2). Those on the forefront of technology start to use MP3 as an alternative to purchasing CDs with music produced by the recording studios. As this is a small number of users and the use of the technology takes a highly skilled individual, the impact to the recording studios is negligible.

A short time later (C_3), we see the introduction of home CD writers. Early adopters pick up the technology (B_3), and those early adopters now have the ability to make perfect copies of CDs purchased from the studios as well as create CDs containing tracks from the MP3 files they own. This music is now as portable as CDs manufactured by the studios and can be used outside the computer systems such as in cars, portable CD players, high-end stereos, or in commercial venues performing music for entertainment.

Over time, the cost of CDW drives falls, as does the cost of CD-writable discs (C_4). Decreased costs drive a widespread market adoption of these technologies (B_4). These consumer-written

discs are interchangeable with the studio-produced discs. They are no longer held by a small group but are mainstream-adopted capabilities.

At point (I_3) CDW technology is available but few have adopted the technology. This produces an environment where future widespread adoption of these technologies by the mainstream population is envisioned. These are therefore known unknowns or uncertainty. Known knowns at I_3 involve adoption of MP3 technology as well as current uses and previous uses and possibilities. Any of those previous interactions are likely to occur as well, at least for a period of time. More recent incidents will likely continue to occur, but non-recent events are unlikely to be seen commonly, if ever.

Prior to I_3, at I_2, we may consider that MP3 technology is available and has begun adoption. But CDW technology is not available. At this point the future of widespread adoption by a mainstream market is unforeseeable; these are unknown unknowns.

At each of these intersection points one can surmise various behaviors, especially policies, which would affect the future direction or speed of the progression of intersections. Congress may consider the capital and labor investments of the studios and consider that those investments are worth protecting. They may undertake behaviors (i.e., policies/laws) that will slow the adoption of technologies capable of reproducing high quality music recordings.

For instance, at point I_3 CDW technology and MP3 technology capabilities exist. A policy limiting the legality of using CDW drives for the purpose of making copies of studio-recorded discs would limit the behavior of adoption. If music cannot be distributed to others, it lowers the utility of purchasing a CDW drive. This may drive further behavior changes on CDW drive

makers and CD disc makers who have a smaller market and may not develop additional capabilities to produce cheaper, faster, and better drives and discs.

One could make an argument here, for or against, the inevitability of capabilities to overtake behaviors. For instance, as time progresses, more people are likely to take on the technologies for other purposes (e.g. file backup rather than music exchange). Once the technologies are available, their use for another purpose is trivial. In this sense, the drive and disc makers still develop incentive for increased capabilities and the behavior becomes easier even if by-passing policies or laws to enable it. This pits the wide spread capability to produce illegal copies of music against the illegality of doing so (but with the unlikelihood of being caught).

Similarly it is easy to make an argument using market forces that capability is developed in response to behavior. Writable CDs are easily turned into a commodity where price is of utmost importance to the consumer. With price as a driver, manufacturers have high incentives to develop additional capabilities to produce significantly lower cost CD-W discs and drives. The behavior driver is a policy of maximum profits by increasing volume of sales.

At each of these points in time, how some behaviors and capabilities will interact is well understood, while others are not. Some intersections themselves can be predicted, even when the interaction is not fully understood. Other intersections cannot be predicted because full knowledge is lacking

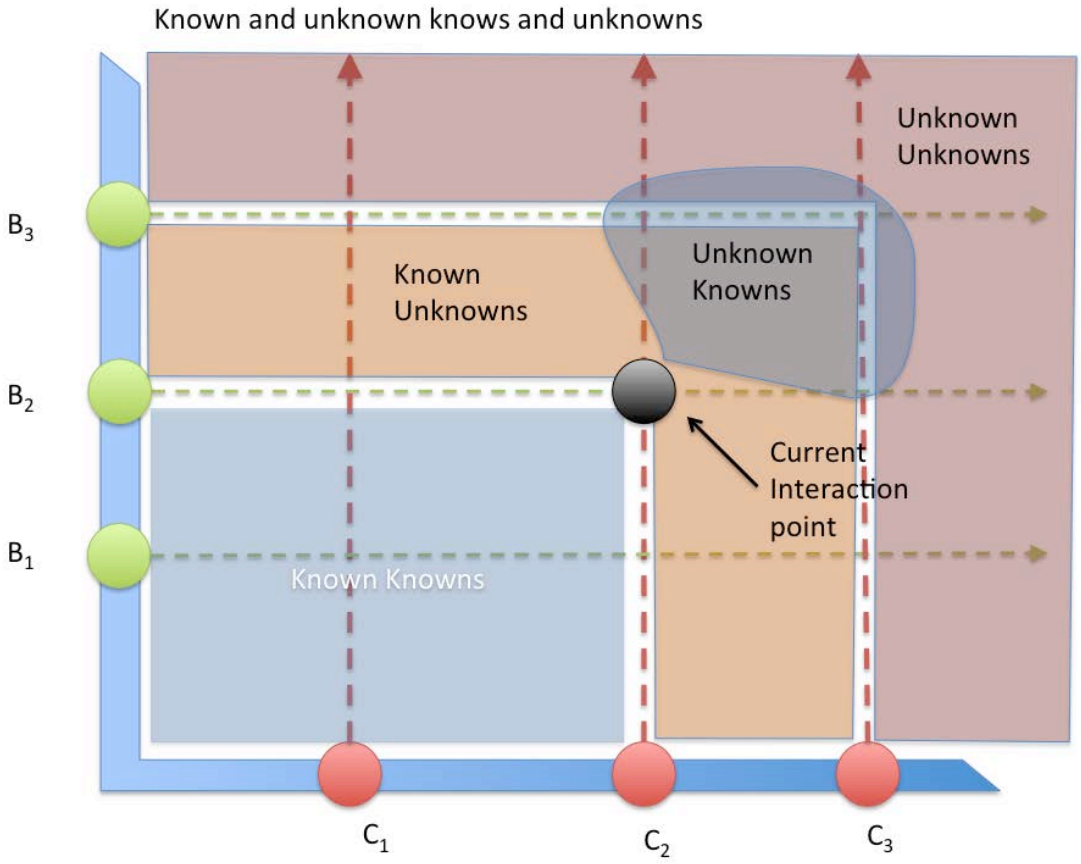

Figure 5

Caption: At any given cyber incident point known/unknown components of behaviors, capabilities, and their interactions/potential future interactions exist. This graphic depicts which sets of behavior and sets of capability are known knowns (combinations of behaviors and capabilities which are known and can be avoided, reconstituted, or tolerated), Known unknowns (that which is not known but we are aware that there is not enough information. Unknown unknowns (can not be predicted from current knowledge, and Unknown Knowns (can be predicted, but we do not believe full information is available for forecasting).

Other Factors

The behavior of a large set of individuals should not be confused with capturing the actions of each individual. While a large population can have fairly predictable behaviors and capability adoption, each individual's adoption of those behaviors and capabilities is distinct and may be difficult to predict. For many cases (e.g., music recording) individuals are irrelevant and considering the whole of a population will produce a better predictive result. For other cases (e.g., the launch of a botnet attack on a cyber component) an individual's actions may have wide-reaching effect and therefore must be considered.

A solution set aligning current and past behaviors to current and future capabilities is in a near constant degradation cycle. In many cases laws pertaining to older technologies are adapted on- the- fly to attempt to fit newer technologies. Applying the 1934 national wiretap laws to modern day voice over IP (VOIP) telephone systems is one example. These existing behaviors almost never match a new capability perfectly, increasing vulnerability due to cyber incidents.

There is potential for behavior cycles as capability proceeds. Prior to CDs there was widespread use of cassette tapes that allowed easy recording of nearly any audio source. When CDs first debut, that recording capability did not exist on the new medium. This caused a change in behavior with the new technology, but over time the recording capability is created for the CD medium, and a return to the previous behavior is seen only at a later capability point. See figure below.

Finally, one must consider whether a set of behaviors itself can constitute a capability. Codification of behaviors through processes or policies may create a capability. A money system is a good example; one person using currency does not amount to a capability, but a million people using the currency enables additional capability compared to the population without a currency.

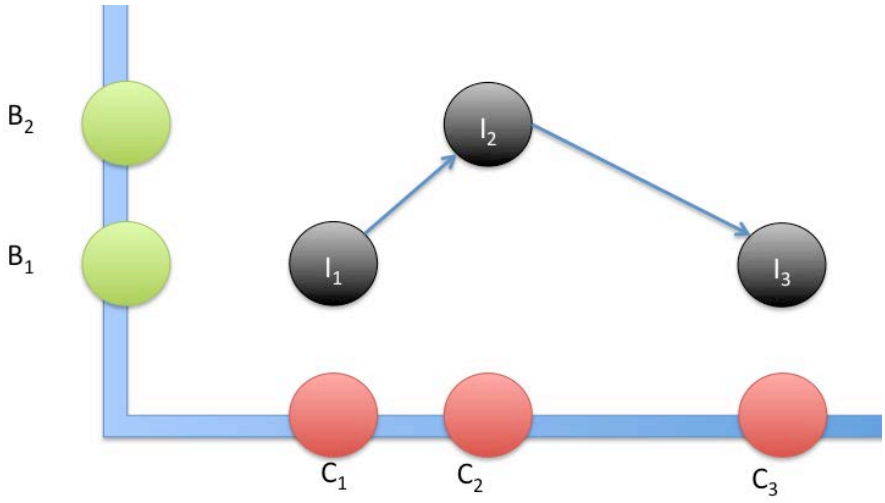

Figure 6

Caption: Behavior cycle: a change in behavior occurs with a new capability. Once the new capability is well understood, the appearance of previous behaviors with updated capability may result.

Section IV: Applying the Framework

Since World War II, the United States has become increasingly dependent on information and communications technology for a broad array of requirements ranging from the availability of clean water to distributing nuclear power. As the United States adapts to the changing landscape of a global economy, it becomes increasingly important to ensure that both government and the private sector work collaboratively to successfully defended resources from cyber attacks, espionage and other threats.

An assessment of current information sharing efforts within the U.S. and its allies, for the purpose of identifying potential shortfalls in the existing information sharing system could provide a road map for future strategies. Experiential knowledge regarding cyber incidents could provide insight into how organizations, government, and academia might change their behavior to resist future threats. A specific focus on how the impact of these incidents drives development of new capabilities and sets of behavior designed to increase security may be instructive in terms of implementations of solutions by developing reporting metrics that inform forecast trends in cyber threats.

Resources Available Now

Leaders responsible for reducing and preventing cyber incidents want technology to support overall mission success, not just IT outcomes. Better use of extensive data assets – harnessing big data – is at the core of how IT can improve the analysis of cyber incidents and aid in the prediction of future events. Only then can behaviors be changed and capabilities developed preemptively to avoid realizing incidents.

As mentioned in the Incident Modeling Methods section of this paper, one such mechanism for tracking cyber incidents is the Index of Cyber Security developed in 2011 by Dr. Dan Geer and Mukul Pareek. The ICS is "a sentiment based measure of the risk to the corporate, industrial, and governmental information infrastructure from a spectrum of cyber security threats. It is sentiment based in recognition of the rapid change in cyber security threats and postures, the state of cyber security metrics as a practical art, and the degree of uncertainty in any risk-centered field. In short, ICS aggregates the views of information security professionals as expressed though a monthly survey."[11]

To produce maximum impact according to the proposed framework, the method of collection must account for behavior and capability changes. The ideal method would attempt to measure the specific changes in behavior and capability independently each month. A mechanism to quantify each factor is required.

Once quantified data is collected, it must be analyzed in a similar way to the ICS. The method must be objective and repeatable as well as transparent. It must provide a mechanism for creating the future prediction zones for behavior and for capability. Higher accuracy in this prediction enables better decision-making as to which behaviors and capabilities should be modified to produce the best coverage against predicted future cyber events.

[11] ICS, http://cybersecurityindex.org

Section V: Conclusion

The Cyber Incident Modeling Framework can be used to examine trends in behaviors and technologies by exploring historical incidents to facilitate understanding of the implications for future incidents. Human interactions in, through, and from cyberspace are common in everyday life. So common that many fail to recognize the growing beneficial dependencies on cyberspace and the corresponding need to make explicit susceptibilities to misuse and the consequences that may occur. To establish a meaningful ability to differentiate between benefit and consequence, one needs a framework to dispassionately assess the nature of *incidents*. The connotation of an incident is an occurrence of something harmful. Cyber incidents are made possible because humans seek a benefit from interacting with cyber capabilities. Cyberspace is an explicitly constructed environment, designed to provide benefit, one could surmise that same design could be applied for consequences as well. Incidents become the observable that indicates that such assessments were either not made or not heeded, but most certainly not countered or mitigated effectively.

Appendix A: The Index of Cyber Security

The Index of Cyber Security is described in full detail at its site. The index is useful as it provides a stable and consistent mechanism for evaluation of cyber security risk while remaining objective and rules based. The Index takes the approach of asking about fifteen areas of cyber security issues and asks participants to rate each on the scale rising fast, rising, static, falling, or falling fast. The survey is repeated each month.

The ICS is consistent in its questions because it wishes to establish an "ongoing, methodologically transparent measure of the state of cybersecurity." The result of this survey is an ad hoc prediction of the future incident prediction zone. Participants know the current set of behaviors and capabilities (or their own interpretation of them) and they understand their own experience of cyber incidents over a recent history. These factors allow for an analysis that is similar, though not identical to the framework developed above.

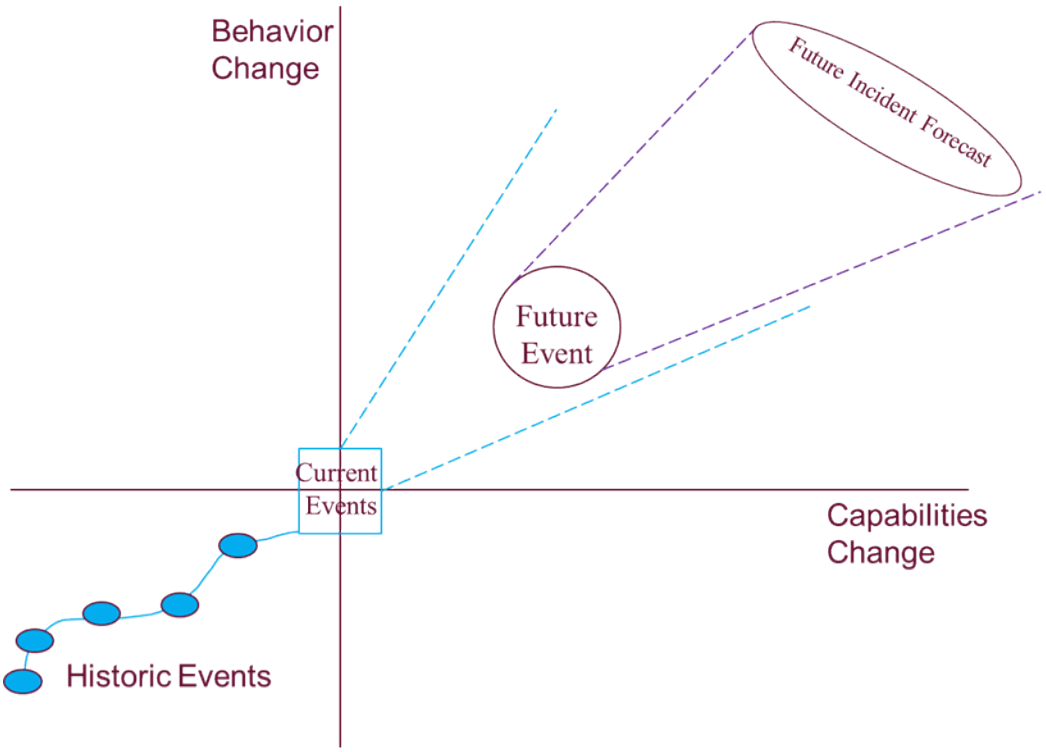

Figure 7

Caption: This diagram shows the predictive power of the Index of Cyber Security.

By combining a recent history of cyber incidents known to the survey respondent with an understanding of the current behaviors and capabilities each respondent is indicating their vision of the future incident forecast. The Index then calculates a combined value. The specific math is available at cybersecurityindex.org.

These prediction and tracking mechanisms are quite valuable and provide a number of features:

- Risk Premiums – In financial markets we see the possibility of beneficial returns on risk. This is not the case with cyber risks where the positive result of investment is that an event is avoided but money was still spent. Thus it is more akin to insurance than a risk management calculation. It is difficult for a cyber risk manager to explain the cost of their actions against a measure of the benefit. The Index enables this type of comparison by the cyber risk manager if similar methods are used.
- Measurement – Financial market risks can be measured and reported using a variety of well-established methods and quantitative tools. Cyber risk is difficult to measure to any quantitative level.
- Non-identical, non-universal asset classes – in financial markets, a dollar is a dollar, and an effect on the price of a single dollar is universal to all dollars. With cyber risks this is rarely the case. A vulnerability in one software version is unlikely to affect another version and very unlikely to affect other software packages.

To produce maximum impact according to the cyber incident framework proposed in this paper, the method of collection must be changed to account for behavior and capability changes. The ideal method would attempt to measure the specific changes in behavior and capability independently each month. A mechanism to quantify each factor is required.

The survey issues in the Index of Cyber Security cover both behaviors and capabilities simultaneously. These must be separated whenever possible so that behavioral and technological changes from month to month can be accurately measured.

Once quantified data is collected, it must be analyzed in a similar way to the ICS. The method must be objective and repeatable as well as transparent. It must provide a mechanism for creating the future prediction zones for behavior and for capability. Higher accuracy in this prediction enables better decision-making as to which behaviors and capabilities should be modified to produce the best coverage against predicted future cyber events.

Appendix B: Attributes of a Cyber Incident

The following attributes are useful to consider as part of a cyber incident. These should be cataloged and analyzed to the greatest extent possible. Other useful attributes exist and should be considered as well.

1. **Attack/Event**
    1. **Effect**
        1. **Consequence**
            1. **Psychological**
            2. **Life Loss**
            3. **Capability Loss**
            4. **$ Loss**
            5. **Consequence Type**
                1. **Intended**
                2. **Unintended**
                3. **Residual**
        2. **Duration**
            1. **Attack length**
            2. **Residual length**
            3. **Recurrence Length**
        3. **Host Affected (graphs can be used here)**
            1. **Cumulative effected over time**
            2. **Currently effected, over time**
    2. **Attacker**
        1. **Motivation [see Cyber index writing "the nature of cybersecurity risks"]**
            1. **Economic**
            2. **Social**
            3. **Political**
            4. **Monetary**
            5. **Military Operation (Cyber-Physical)**
            6. **Intelligence**
        2. **Geographic Location(s)**
    3. **Victim**
    4. **Date**
        1. **Time**
    5. **Type**

    1. **Cyber Physical**
    2. **Cyber Human**
    3. **Cyber Malicious**
    4. **Proof of Concept**
    5. **Accidental**
6. **Method**
    1. **Path to target**
    2. **Method Sophistication**
        1. **High**
        2. **Medium**
        3. **Low**
    3. **Cyber Attack Threat**
        1. **Social Engineering**
        2. **Network Sniffers**
        3. **Packet Spoofing**
        4. **Session hijacking**
        5. **Cyber-threats and bullying**
        6. **Automated Probes and Scans**
        7. **GUI intrusion tools**
        8. **Automated widespread attacks**
        9. **DOS and DDOS (denial of service) attacks**
        10. **Industrial Espionage**
        11. **Executable code attacks (against browsers)**
        12. **Analysis of vulnerabilities in compiled software**
        13. **Widespread attacks on DNS infrastructure**
        14. **Widespread attacks using NNTP to distribute attack**
        15. **"Stealth" and other advanced scanning techniques**
        16. **Windows-based remote access trojans (Back Orifice)**
        17. **Email propagation of malicious code**
        18. **Wide-scale trojan distribution**
        19. **Distributed Attack Tools**
        20. **Targeting of specific users**
        21. **Anti-forensic techniques**
        22. **Wide-scale use of worms**
        23. **Sophisticated botnet command and control attacks**
7. **Target(s)**
    1. **System**
    2. **Exploited Technology**
    3. **Category**
    4. **Version**

8. **Attack Sophistication**
    1. **High**
    2. **Medium**
    3. **Low**
9. **Proves concept (enables future attack)**
10. **Zero day attack**
11. **Availability of solution before attack**
    1. **Measures of adoption**
12. **Origin of Exploit**
    1. **Military**
    2. **Research Lab**
    3. **Vendor**

2. **Actors**
    1. **Attacker(s)**
    2. **Victim(s)**
    3. **Generic Actor profile**
        1. **Mission**
        2. **Name**
        3. **Resources**
            1. **# of people**
            2. **$ of resources**
        4. **Category**
            1. **Nation state**
            2. **Individual**
            3. **Corporation**
                1. **Fortune 1000**
                2. **Mid-size**
                3. **Small**
            4. **Non-state actors**
        5. **Knowledge, Skills, and Abilities**
        6. **Available tools**
            1. **Cyber**
            2. **Physical**
        7. **Policy (might bring in from SCRM trees)**
        8. **Geographic Locations**

3. **Response**
    1. **Lessons Learned**
        1. **Change in Posture**
        2. **Future Active Defenses**
        3. **Plans for Future Policy**

    4. **New Entities Created**
2. **Speed of Solution**
    1. **Unresolved Issues**
    2. **Ongoing Effects**
    3. **Total Mitigation Efficiency**
3. **Jurisdiction**
    1. **International Engagement**
    2. **State/Local**
    3. **DoD**
    4. **Other Government**
4. **Political Fallout**
    1. **Use of Existing Policies**
    2. **Discover of Policy Voids**
5. **Originator of Response**
    1. **Private Sector**
    2. **Government**
    3. **Individual**
6. **Ability to Punish Perpetrators**
    1. **Court Cases**
    2. **Fines**
    3. **Imprisonment**
    4. **War**
    5. **Retaliation**
7. **Cost**
8. **Attribution**
9. **Use of Existing Defense**
    1. **Knowledge of Vulnerabilities**
    2. **Cyber Work Force**
    3. **Active Defenses**
10. **New Policies resulting from Attack**

Appendix C: References

Alperovitch, Dmitri. “Revealed: Operation Shady RAT”. McAfee Threat Research. 2011

Bari, Afzal and Helen Domenici. “The Price of Cybersecurity: Big Investments, Small Improvements”. Bloomberg Government Study. January 31, 2012.

Defense Security Service. “Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry”. 2011.

Department of Defense- Defense Industrial base Voluntary Cyber Security and Information Assurance Activities. Interim Final Rule. http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf. April 30, 2012.

Friedman, Allan. “Economic and Policy Frameworks for Cybersecurity Risks”. Brookings, Center for Technology Innovation. July 21, 2011.

Grauman, Brigid. “Cyber-Security: The vexed question of global rules”. Security and Defence Agenda Report. February 2012.

Lord, Kristin and Travis Sharp. “America’s Cyber Future, Security and Prosperity in the Information Age”. Center for a New American Security. Volume 1. June 2011.

Lord, Kristin and Travis Sharp. “America’s Cyber Future, Security and Prosperity in the Information Age”. Center for a New American Security. Volume 2. June 2011.

“Project Enlightenment: Overview of Modern Cyber Espionage in a Global Economy”. Cyber Squared Inc.

Shimeall, Tim, and Phil Williams. "Models of Information Security Trend Analysis." CERT Analysis Center, Software Engineering Institute. April 16, 2012 <http://202.41.82.144/data/HACKING_INFORMATION/PRINTED%20PAPERS/models%20for%20inf%20security%20TREND%20ANALYSIS.pdf>.

United States General Accounting Office. “Virus Highlights Need for Improved Internet Management”. Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives. June 12, 1989.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
June 2012	Paper	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Framework for Cyber Incident Modeling	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Cameron DePuy, Brendan Farrar-Foley, Rachel Greenspan, Gilbert Watson III John Thompson	5e. TASK NUMBER CRP C5139
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Nonstandard Document NS D-4658 Log no. H 12-000950

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; unlimited distribution: 28 June 2012.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper proposes a framework to identify the history and current state of cyber incidents and lay the groundwork to forecast "future cyber history." Analysis of current cyber incident reporting is hindered by the inconsistency of data fields. There are numerous underutilized data sources of recorded cyber incidents. This paper proposes a cyber incident analytical framework that will first offer a taxonomy for cyber incidents. This allows establishing a common incident lexicon to transform multiple sources of data into a comparable form. By building a framework that defines common parameters, multiple sources of incident reports may be equalized and compared across many dimensions (e.g., time, locality, industry sector, attack type). A cyber incident is an observed risk that can be decomposed into two main components: susceptibility and consequence of impact. Susceptibility may be further broken down into known threats and known vulnerabilities. The consequence of the cyber incident that occurred is measurable in terms of cost, schedule, performance, and the change in behaviors. Trends can be determined by observing the resultant changes in behavior and capabilities from historical data. The change in technology/capabilities and the change in behaviors over time can then be used to forecast and provide insights into forecasting a "future cyber history." The proposed analytical framework helps to define, discover, and learn from past cyber incidents to drive future capabilities and future behaviors to better detect and respond to cyber incidents.

15. SUBJECT TERMS

Cyber Incident, Cyber Forecasting, Behavior Change, Capability Change, Framework

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified					Cameron DePuy
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclassified	Unclassified	Unclassified	Unlimited	38	703-845-6679