MP 180673
MITRE PRODUCT

MITRE

Foundational Concepts for Quantifying Asymmetric Non-Kinetic Threat Vectors

Project No.: 10AOH810-JF

Lexington Park, MD

Authors:

F. Lynam
L. Oringer

Peer Review:

P. Polmonari
R. McInnes
M. McFarren
A. McEachron

October 2019

Abstract

This paper provides a means to characterize asymmetric threat vector problems (such as adversarial activity against a supply chain or in the cyber domain) in terms of formal modeling techniques. This characterization is used to provide a foundation for how to structure empirically-based analysis in these domains in a consistent and useful manner. This paper is intended for analysts who want to develop actionable assessments for asymmetric threat vectors, such as cyber security, supply chain security or other systems security analysts. This paper provides clear delineation between deterministic, stochastic and agent-driven elements of asymmetric threat vectors, distinctly defining the functional differences between concepts such as vulnerability and threat, and argues that traditional game theory approaches should prove inherently inefficient for these types of problems.

Overview

Asymmetric threat vectors can provide otherwise symmetric adversaries with low-investment means to undermine our high-investment systems. Non-kinetic threat vector spaces, such as cyber, supply chain or insiders, have the potential to be used to execute kinetic impacts, such as physical damage, at a lower investment than otherwise symmetric kinetic threats. These threats cannot be adequately managed by classical risk analysis methods, and require additional features to address the special considerations of adversarial decision making.

Traditional risk management, such as in manufacturing or safety critical system failure analysis, focuses on the interaction of spontaneously probable events and their consequences. Agent-driven risks, such as kinetic or non-kinetic threats, are not spontaneous. These risks come from sophisticated investments selected by highly intelligent actors. This paper places agent-driven risks against a contextual background of modeling traditional risks in order to provide a foundation for defining acceptable criteria for analysis to mitigate agent-driven asymmetric threat vectors.

Reliability Risk Analysis

A risk is the possibility of an undesirable outcome. Risk can be expressed in terms of the expectation value for a particular scenario, which is the mixture of the probability and the impact of a given undesired outcome. For example, when looking at parts reliability in safety of flight, risk is expressed as a relationship between likelihood and consequence of random part failures. We can formally capture this relationship in terms of mathematical and logical functions using different types of models. Models are a way to describe systems. They themselves represent our understanding of a system in explicit terms, an understanding which can be evolved as information is gained.

Consequence is modelled as a deterministic process: if the wing falls off, the plane will crash; if a coin lands heads, I lose. Models meant to analyze risk must incorporate deterministic relationships between specific events and some unwanted condition in order to convey impacts. Deterministic processes exhibit small-scale consistency, where each step is well understood and can be precisely anticipated.

Likelihood, for these kinds of spontaneous processes, is also deterministic: a wing spar fails because of a pre-existing manufacturing flaw; a coin lands heads because of the subtle physical preconditions of the coin toss. However, these example systems, while their outcomes might fall into well-defined bins, are often chaotic: they contain variations too small to observe reliably but large enough to influence which outcome occurs. It's theoretically possible to perfectly predict the specific outcome if you know all of the data about a system, but in practice it's nearly impossible to know all of the data about a real system.

Fortunately, deterministic systems behave deterministically whether or not you know their hidden variables. Although failure rates and coin flips appear chaotic, they are still behaving deterministically below the observable level. Small-scale consistency produces large-scale consistency, and those hidden variables appear to have consistent distributions of possible values. This means that even seemingly chaotic systems behave in an anticipatable manner, allowing stochastic models to make useful probabilistic predictions about them. For example, we can assert the odds of obtaining a heads in a coin flip is 1 in 2, or the odds of rolling a six on a die is 1 in 6. Even though we cannot deterministically demonstrate the coin will not land heads, we can still make informed decisions by knowing that, when compared to rolling a six, the risk imposed by the coin flip is greater.

We can use reliability and historical data to characterize the time between particular failures. Much like the coin flip, we can then connect that stochastic model of failures with the deterministic model of the impact. Imposing formal and empirically-based structure to the construction and evaluation of models of these behaviors ensures well-bounded coverage of the problem space.

Reliability risk is about the probability of spontaneous bad things: a stochastically induced deterministic event; likelihood acts as an input to consequence. Additional considerations are necessary, however, to account for agent-driven risks.

Non-Kinetic Threat Vectors

Threat-driven risks are not spontaneous and instead contain agents which selectively choose to induce the failure or risk realization process. In lieu of the simple combination of likelihood and consequence found in analyzing parts reliability, threat-driven risks are often described in three terms: threat, vulnerability and consequence. Vulnerability and consequence can be properly described by the same stochastic and deterministic models as in reliability analysis as above, respectively, but threat is an agent-driven process and must be handled appropriately.[1]

Consequence in this model remains observably deterministic. Vulnerability, in contrast, lacks a consistent definition that would support use of a stochastic model. This is an important nuance which illustrates a general inconsistency in the functional usage of the concept of "vulnerability." For example, the cyber community uses the term "vulnerability" to describe known software design flaws. However, once these flaws are known to exist and have known operational outcomes, they are deterministic consequences of exposure to the adversary and are effectively a consequence of said exposure. However, in the characterization of risk, there must be some term that captures the odds that an agent-driven process (threat) would be able to find and successfully execute the sequence of steps required to induce a particular consequence by discovering and exploiting a series of individual system design flaws present but not yet known. This is the underlying nature of the stochastic term in a threat vector model, which can be considered as the functional intent of the term "vulnerability" here. A system is more vulnerable to a more capable adversary: being able to identify novel exploitable flaws faster means the odds of their discovery over a given time are higher.

Notably, the structure and interconnection of the physical, logical or human system is itself a deterministic part of the representation of reality, traversed by an agent via methods whose reliability is sometimes chaotic and whose path is potentially unknowable. For an agent-driven risk, the stochastic elements of the system simply present an attack surface which connects the decisions of the agent to the deterministic outcomes, via the probability of successfully obtaining that outcome. The threat term is the agency in this model. Threat is neither deterministic nor stochastic, it doesn't act consistently on a small scale and it doesn't act consistently on a large scale: it is unknowable.

This inherently unknowable, adaptive agent is the input term in a non-kinetic threat vector risk model. A full and complete understanding of consequence and vulnerability, the deterministic and stochastic dimensions, cannot alone make useful predictions about which path an adversary will take to induce a failure. However, anticipating the specific choices an adversary will make is not effective nor sufficient to address asymmetric threats in the non-kinetic threat vector space, because as threat is an adaptive

[1] "Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, January 2013

agent, those choices can explicitly depend on how well you've anticipated them. Defense against an intelligent agent is only effective so long as it leaves open no comparably viable alternatives open to the offense.

Applying Agency Models to Asymmetric Problems

In contrast to random failures, adversaries make decisions, often following rules or doctrine. This agency is often modeled using game theory, applying intelligent optimization strategies or iterative machine learning solutions which lend reasonable credit to a competent adversary who can respond adaptively to move and counter-move. However, anticipating the adversary's choice of decision making policy is not relevant to the goal of reducing the risk of exploiting asymmetric threat vectors: the presence of available threat vectors presents a measurable risk regardless of what choice the adversary might make at any given moment: if the door and the window are open, the adversary will take the door, close the door and the adversary will take the window. Both should be identified explicitly in a single computation so that common solutions can be explicitly assessed, something traditional game theoretic approaches often lack.

Kinetic threat vectors can be leveraged to impose a cost on the adversary to match a symmetric capability or counter-capability. This cost imposition deters adversary investment, often because the cost of any successful investment could exceed the benefit gained. Non-kinetic threat vectors can present an asymmetric means to undermine the effectiveness of this cost imposition deterrence.

The effective means to counter asymmetric threat vectors, therefore, is not to anticipate the particular means the adversary will select, but to change the deterministic or stochastic elements of the system to increase the cost imposed for all available options until no cost-effective asymmetric threat vectors remain. Non-kinetic threat vector risk analysis must aim to "raise the bar" beyond the cost of reaching parity through a kinetic arms race.

If we spend a billion dollars developing a capability, it should cost the adversary a billion dollars to level the playing field, whether they chose to do so by investing in a comparable development or by denying us effective capability through other, non-kinetic means. The particular option an adversary might select is irrelevant: no option can be left available that provides an asymmetric advantage.

For non-peers against whom we pose an existential threat that they cannot directly counter, inducing denial of those threats is a clearly distinct option from developing symmetric capability in an important way. The potential value gained by denying your adversary a capability that poses an existential threat to you is only limited to within the level of investment that would itself pose a comparable threat. For our own capabilities which pose existential threats to others who lack symmetric options, adversary investment even beyond the cost of those capabilities themselves could be rationally justified.

For our peers with symmetric capabilities which pose mutual existential threats, their ability to deny the effectiveness of our capabilities poses an exceptionally grave concern. Even a symmetric risk which threatens to deny our key strategic capabilities undermines, or even eliminates, the effectiveness of the mutually assured destruction doctrine. Investment in assurance against the non-kinetic denial of strategic capabilities is an existential concern.

Reducing Asymmetric Disadvantage

A well-structured modeling formalism for the deterministic and stochastic elements of non-kinetic threat vectors must provide a means to account for all potential options available to an adversary. While the specific choices an adversary will make may be unknowable in advance, the only option available to defend non-kinetic threat vector terrain (defined as both human and cyber systems) is altering the knowable elements which facilitate asymmetric risks, such as the structure of the terrain itself (to include the level of foreknowledge available about that structure). This is the defender's mechanism to drive the cost imposed to execute successful offensive options past an adversary's capacity for investment.

Reducing asymmetry disadvantage in the non-kinetic threat vector space can be accomplished efficiently through an understanding of the interaction between threat, vulnerability and consequence. Based on the understanding set forth above, we can clearly leverage existing concepts in risk analysis to tackle the deterministic, stochastic and agent-driven parts of the non-kinetic threat vector problem . Resilience is any effect which modifies deterministic processes, reducing consequence. Security is any effect which modifies probabilistic processes, reducing vulnerability or likelihood. Deterrence is any effect which modifies agent-driven decision-making processes, reducing the threat.

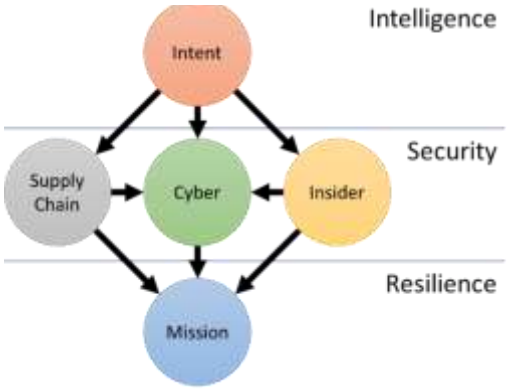
The objective of design basis analysis must be to alter the design and operation of the system sufficiently to deter attempted initiation of any non-kinetic threat vector. For example, building a resilient and secure system that is challenging to compromise can deter investment in defeating a system. The effectiveness of any particular response to reduce the viable attack surface can thus be determined by the relationship between the deterministic and stochastic models, and where that places the minimum threshold for a credible adversary effect.

As discussed above, the threat agent is inherently adaptive and asynchronous, making iterative assessment via application of traditional game theory an inefficient and potentially ineffective means to address asymmetric threats.[2] A formal construct is required which supports addressing the complete space of asymmetric threat options in the absence of a particular adversarial strategy, and which makes no assumptions about the choices to be made by an adversary that can and will adapt and overcome.

[2] G. Wyss, J. Clem, et al, "A Method for Risk-Informed Management of Enterprise Security (RIMES)," Sandia National Laboratories, October 2010

Applied Asymmetric Problems

Figure 1 - High Level Graph of Applicable Non-Kinetic Threat Vector Space



The relevant asymmetric non-kinetic threat vector space can be notionally described by the figure on the right, where non-kinetic activities are leveraged to bridge some adversarial malicious intent and some mission impact. An exhaustive description of the bounds of this graph should provide limitations on the scope of potential asymmetric non-kinetic threat vector spaces. This becomes the interaction of some stochastic "red process" describing how an adversary can traverse vertically down this graph to compromise some deterministic "blue process" describing normal or desired operations in the mission space.

Asymmetric effects of significance today span three threat vector spaces: the supply chain, cyber space and insiders.[3] The supply chain can be considered an intendent blue process within the supply chain sub-graph, resulting in a recursive application of this model in characterizing the problem space with additional mission, supply chain, cyber and insider sub-graphs. Additionally, the cyber space on this graph should be considered to encompass both traditional information technology as well as operational, or cyber physical, technologies. Traditional information technology is commonly associated with data exfiltration effects (which can be mission defeating), whereas operational technology (to include electronic warfare-derived interfaces into cyber systems) can result in damage to equipment or personnel with more immediate or explicit mission impact. As humans are intrinsically an element of our socio-technical systems, insiders pose a risk of adversarial engagement within otherwise trusted spaces for both of these other effect areas that can and should be modeling accordingly.

Conclusion

Asymmetric threat vectors consist of deterministic, stochastic and agent-driven elements. Mature methods and approaches exist to characterize these kinds of problems, and should be employed in a manner which explicitly draws the distinction between each element of the threat vector. Importantly, asymmetric threat vectors are not a traditional turn-taking game, and alternative analysis approaches which address the multi-path, multi-step and multi-target nature of asymmetric effects must be employed to provide effective analysis of asymmetric threat vector problems.

[3] C. Nissen, J. Gronager, R. Metzger, H. Rishikof, "Deliver Uncompromised," The MITRE Corporation, August 2018