MESSAGE FROM THE DIRECTOR

The first part of this year is shaping up to be almost as eventful as 2020. While vaccines have slowed the spread of COVID-19 in the United States and other Western countries and given many the hope of returning to some kind of normality, the pandemic rages on in places like India and Sub-Saharan Africa. At the same time, we have witnessed some striking incidences of emerging threats. Two of the most glaring examples in the United States were the unprecedented assault on the U.S. Capitol on January 6 and the ransomware attack that shut down the Colonial Pipeline – and fuel supplies to much of the Eastern United States – on May 7. What ties these two events together is that both were surprises that should not have been. The growing agitation of adherents to far right conspiracies such as QAnon and the vulnerability of critical infrastructure to cyber-physical attacks have been prominent talking points amongst the security establishment for several years. Yet it seemed as if those entrusted with protecting the Capitol and the pipeline did not adequately prepare for or defend against these threats. In each case, there were no doubt individual and organizational biases that prevented leaders from adequately understanding or countering the threat – and there is no evidence that either of the target institutions utilized any rigorous form of Red Teaming to counteract these biases and draw attention to their defensive deficits. At the risk of preaching to the choir, these two cases alone should justify an expanded use of Red Teaming for both physical and cybersecurity. As members of the Red Teaming community it is incumbent upon all of us to bring the benefits of Red Teaming to the attention of decision-makers, but we need to do so without a scolding or self-righteous attitude, in a manner that highlights the value of Red Teaming and makes it less intimidating to potential users.

Returning from the larger risk environment to the humbler activities of CART, the Center has been involved in a number of efforts over the past few months, from our “Infectious Incentives” strategic simulation to experiments analyzing how different types of participants produce different Red Teaming outcomes. As these projects wrap up, we will share their results in future newsletters, but I did want to draw everyone’s attention to a new initiative that we are undertaking. We have had a lot of interest from various people in the Red Teaming community about participating in our exercises and research, and have also needed to identify some pretty specific subject matter expertise for some of our simulations (which is sometimes difficult to do on short notice, even when we can compensate people). The solution devised by our resourceful staff is to create a database of Red Teamers, where we can maintain a go-to roster of persons interested in participating in Red Team exercises, together with information about their expertise and knowledge. See the Spotlight on the last page of this newsletter for instructions on how to sign up. We invite anyone who is interested in working with CART in the future to share their details, which we will, of course keep secure. (Red Teaming the security of this database will be a project for our Fall student interns!).

Wishing you success in all your Red Teaming (ad)ventures!

Sincerely,
Gary Ackerman
Director, CART
Premortem analysis allows red-teamers to identify critical flaws in a decision before it is implemented by visualizing what failure looks like. In a premortem, a team imagines failure and then works backward to determine what could lead to failure. The journal article Rubicon Theory of War (Johnson & Tierney) warns that developing an implemental mindset can lead to overconfidence — certainly an undesirable characteristic when a decision involves national security issues. An implemental mindset narrowly focuses on a chosen path accomplishing a desired outcome while avoiding reviewing alternative ways to achieve success.

Premortem analysis is a cognitive tool which challenges the premise that a decision achieves a successful outcome by claiming that the decision has failed miserably. It breaks away from the mental models that develop the implemental mindset and enables red teams to use critical and creative thinking to conceive of how the decision can fail. The critical vulnerabilities exposed by utilizing premortem analysis will help red-teamers develop mitigation signature steps to make the decision more adaptive and resilient.

The signatures produced with PA by red teamers are interpretations of anticipatory analysis of the complexities surrounding our national security issues. Stated simply, complexity arises where an increasing number of independent variables interact interdependently and unpredictably in a similar manner to complex adaptive systems. Dr. Gary Klein’s Harvard Business Review article, Performing a Project Premortem, discusses how research that uses prospective hindsight (aka premortem analysis) increases the ability to identify reasons for future outcomes by 30 percent. This increase considerably helps visualize the implications of failed decisions, which gives a person, group, or organization a conceptual framework to make improvements on the decision before it is put into action.

Premortem Analysis allows red-teamers to visualize failure, which disengages the implemental mindset and develops other options to be challenged. When a decision has direct impact on people's lives, the premortem analysis is an effective tool to challenge that decision before implementation. A key component in the formula of success through the eyes of failure is developing visualization goals for decision making. The visualization goals mitigate a person's or group's overconfidence, which allows for a higher chance of achieving a successful conclusion.

In summary, Premortem Analysis helps avoid an implemental mindset, reduces overconfidence in the team, enables creative thinking, exposes vulnerabilities, and strengthens confidence in your planned program.
RED TEAMING DISPATCHES  JANUARY - MARCH 2021

General
Why Red Team Testing Rules the Cloud, Security Intelligence (January 7, 2021)
You Need a Red Team, Prelude (January 11, 2021)
Virtual Wargaming: Tips and Lessons Learned, Georgetown University Wargaming Society (January 19, 2021)
So You Want to Be a Red Teamer?, SANS Offensive Operations (January 21, 2021)
Edwards Air Force Base Breaking Ground Soon on New Joint Simulation, KGET (February 16, 2021)
Is the Department of Defense Making Enough Progress in Wargaming?, War on the Rocks (February 17, 2021)
Red Teaming/Adversary Simulation Toolkit, Github (February 17, 2021)
This is Not a Drill: Designing Tabletop Exercises to Test Your Prevention Strategies, JDSUPRA (February 18, 2021)
An Introduction to Red Team Assessments, Payatu (March 17, 2021)
#StateoftheHack: Extortion, Ransoms and the Wonderful Life of Red Teaming, Mandiant (March 18, 2021)
Defense in a Competitive Age, UK Ministry of Defense (March 21, 2021)

Exercises
Information Warfare Capabilities Demonstrated at Table Top Exercise, Air Combat Command Public Affairs (January, 2021)

Media Articles
The Marine Corps Expect to Break Ground on a State-of-the-Art Wargaming Center in 2021, Marine Corps Times (January 11, 2021)
Marine Corps Establishes Cyber “Blue Team” Designation, Military Spot (January 21, 2021)
Pentagon to Include Climate Risk in War Games, The Hill (January 27, 2021)
How to Effectively Conduct Remote Crisis Simulation Exercises, Grant Rayner (February 2, 2021)

SPOTLIGHT  Experts Wanted!

Check out our new Expert Registration form if you are interested in signing up to be a potential participant in future CART Red Team Exercises!