2020 | Q4

THE RED SIREN
Quarterly Newsletter

MESSAGE FROM THE DIRECTOR

New Year’s greetings to all! In early November, the United States experienced one of the more consequential and contested elections in recent memory. Although the vote and its aftermath demanded most of our attention, in the small corner where us Red Teamers scheme, CART celebrated its one-year anniversary. This allowed our team to take a step back and evaluate what we have accomplished in our first full year of operation.

In keeping with Red Teaming best practice, when making any evaluation of our performance we should take stock of the many biases that we are subject to – from personal interest bias and groupthink to base-rate fallacy and confirmation bias. We therefore fully acknowledge that our judgment in this is far from objective. Nonetheless, we still believe that CART’s progress has been remarkable, all the more so given that our first year’s activities were conducted during a pandemic and conditions of deep-rooted societal instability.

Among CART’s achievements over the past year:
- Conducted six major Red Teaming exercises, four involving more than 100 participants each.
- Received funding for four substantial research projects involving Red Teaming.
- Developed new Red Teaming concepts and formats, including Course of Action Red Teaming, Strategic Dynamics Red Teaming and an online Red Teaming Experimental Platform.
- Assembled a distinguished Advisory Board consisting of 11 leading practitioners and thinkers in the Red Teaming space.
- Published several reports and articles and featured in several news stories, including in Jane’s International Defence Review and CBRNe World.
- Initiated an internship program that has so far worked with over 30 undergraduate and graduate students.
- Established strategic partnerships with more than ten prominent entities working in the Red Teaming and related domains.

None of this would have been possible without the enduring support from our College and University, our Advisory Board, our wonderful team of Research Assistants and you, the Red Teaming community. We wanted to take this opportunity to thank the broader CART family for making our first year one to remember.

We look forward to continuing to engage with and learn from all of you and to growing the science and practice of Red Teaming. And of course, to a more peaceful and safer 2021.

Sincerely,
Gary Ackerman
Director, CART

albany.edu/cehc/cart   SUBSCRIBE   cart@albany.edu
Collect as much information as possible about the target. A critical preliminary step in Red Teaming is gathering thorough information on as many aspects of the targeted entity as possible, including such aspects as its infrastructure, operations, stakeholders, defenses and competitors. Of particular importance is understanding where the entity places the most value, i.e. its “crown jewels”, since this will differ across targets. This has been recommended by several sources, but there have been no direct empirical tests in the literature [3 sources].

The Red Team must be involved in all stages of an effort, from initial planning through implementation and reporting. This ensures that crucial Red Team principles are considered during both the design and conduct of an exercise or penetration, and allows for alternative analysis to play a role throughout. There appears to be consensus in the Red Teaming literature, although there has been no empirical validation [4 sources].

Perspective

CRAFTY BASTARDS DO THINK DIFFERENTLY: SEEING WHAT IS HIDDEN IN PLAIN SIGHT, INVISIBLE TO THE UNTRAINED EYE

Kathleen Kiernan, Ed.D - CEO, Kiernan Group Holdings Inc. and CART Advisory Board Member

What exactly does a pickpocket, musician, gamer, firefighter, comic book writer, commodities trader, Navy SEAL, Bush pilot and dance instructor have in common? It is not a trick question and the answer is simply that they have more in common than you think. Enter Furciferi Versuti®, AKA Crafty Bastards, a convergence of talent earned by masters of their trades (who except for one, are disconnected with any aspect of homeland or national security), to uncover and undermine the threats posed to it. This effort emerged following an analysis of the outcomes of national exercises, which tended to yield consistently predictable and thus less useful results. Interestingly, it was not a lack of expertise that was to blame for this - it was the direct result of similar shared expertise. We re-learned what we already knew: that administrative and bureaucratic structures can inhibit innovation, create self-induced constraints and doctrinal locks in a battle against adversaries free of such constriction. Sometimes experienced personnel need official permission to color outside the lines and seriously consider the art of the outlandish or outrageous.

Today’s threat landscape is continually changing and is increasingly complex, amplified when the enemy and their tactics are disguised or unknown. Potential and emerging threats can be seen in: the blurred outlines of the proliferation of violent ideology and extremism measured by the public display and the leakage of an underlying but palatable rage; shifts in the global economy which intensify regional resource constraints and access for many to needed medical assistance; increased successful coordinated cyber-attacks; and expanded global criminal networks, among others. Countering these threats and the complex problems that stem from them requires the development of novel approaches.

Crafty Bastards provide new lenses through which to view the world, illuminating dangers embedded in plain sight. They differentiate adversaries from potential allies amid the chaos of broad social and political change, and expand the collective capacity to respond in the face of complex problems in more versatile, more creative, and timelier ways. This variety and depth of skills allows for the overlay of unique perspectives, while accounting for diverse cultures, context, and tactics in the analysis and development of actionable solutions. Our approach includes 18 separate, non-linear, non-kinetic lenses to examine and exploit key assumptions. You can find the Crafty Bastard Playbook by clicking here:

Steve Jobs was initially reluctant to send one of his most senior innovators, and I suspect because the construct was so closely aligned with his worldview, thankfully, he yielded. In tribute:

“Here’s to the crazy ones. The misfits. The rebels. The troublemakers. The round pegs in the square holes. The ones who see things differently...Maybe they have to be crazy. How else can you stare at an empty canvas and see a work of art? Or sit in silence and hear a song that’s never been written? Or gaze at a red planet and see a laboratory on wheels? We make tools for these kinds of people. While some see them as the crazy ones, we see genius. Because the people who are crazy enough to think they can change the world, are the ones who do.” ~Steve Jobs

What have we learned from our Crafty Bastards plank holders? Here are a few key takeaways: the capability to divert attention and manipulate that space and time; the recruitment of musicians resembles a HUMINT operation; comic books can be used in Influence Operations; Bush pilots can see with their ears and listen with their eyes, and firefighters can identify concealment techniques from chasing the movement of smoke. Navy SEALs, well, we will leave those lessons in the quiet space behind the curtain.
The election and its aftermath proved to be just as contentious as many had anticipated and, as noted in the previous newsletter, was subjected to a fair amount of Red Teaming. Beyond the much-publicized Transition Integrity Project wargame on the outcomes of the election, there were also Red Teaming exercises to protect against disinformation and test the security of voting machines.

- **RSA Red Team Exercise Highlights Election Threats from Deepfakes and Fake News**, TechRepublic (February 26, 2020)
- **Election War Games Show Cyber Chaos Doesn’t Cost Much**, SDX Central (August 24, 2020)
- **The United States Needs a Red Team to Protect the Election**, Foreign Policy (October 15, 2020)
- **How Hackers Could Take Down the Election...or Save It**, Freethink (October 21, 2020)