Cyber (In)Security: Decision-Making Dynamics When Moving Out of Your Comfort Zone

Andy Cohen

"Every assumption we hold, every claim, every assertion, every single one of them must be challenged."[1] —General Mark A. Milley, 39TH Chief of Staff of the U.S. Army

OVERVIEW

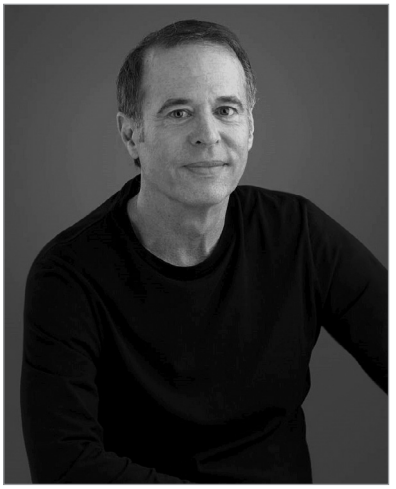
This paper focuses on how the dynamic speed of change and the compression of time in cybersecurity move individuals and organizations out of their comfort zones. This often results in forcing faulty decision-making generated by an enhanced dependence on untested assumptions. The counterbalance to this behavior begins by recognizing a key truism: within every decision lies an assumption. Equipping your cyber team with the mechanisms and tools to identify and properly challenge these assumptions drives better decision-making and new opportunities to successfully defend, attack, and adapt in the cyber battleground.

Making Decisions Outside Your Comfort Zone

Aron Ralston, the hiker forced to sever his own arm after it became stuck between two rocks and the inspiration for the film *127 Hours,* admitted that his greatest fear throughout the entire ordeal was having to get a shot at the hospital. Needles made him uncomfortable.[2]

Orville Wright, one of the two brothers who ushered in the art of modern aviation by inventing and flying the first plane, dismissed the idea of creating a runway that smoothed over the rocks and debris on the airfield. In his eyes, if a man had to smooth over every takeoff strip (which today is called a tarmac), he shouldn't be flying. Investing in a tarmac seemed silly to him.[3]

Houdini was the king of escapes—nothing could hold him back. Yet when riding with a friend in a new car, he couldn't open the door on his own because the door handle was in a different place than the one on older models. Joked Houdini, "I've escaped



Andy Cohen is an entrepreneur, best-selling author, and international thought leader. His keynotes and workshops are world-renowned and include appearances at the Army Cyber Institute, Google, HSBC China, and The World Bank. He has a degree in experimental psychology and a room full of prestigious advertising awards for finding creative solutions that drive measurable sales. Andy is the Chief Assumption Officer of Andy Cohen Worldwide, a global advisory firm helping multinational businesses as well as small firms make faster, better decisions. Between engagements, Andy teaches at the world's most respected universities including New York University, Duke University's Fuqua School of Business, UC Berkeley, ISB (India), and CKGSB (China). *Follow the Other Hand,* Andy's first book, was a *New York Times* notable book. It has been translated into multiple languages. Colonel (Ret.) Greg Conti, Ph.D. called Andy's newest book, *Challenge Your Assumptions, Change Your World,* a must-read for the security professional."

from practically every type of a container and every size, shape, and weight of boxes, trunks, and other such things, but I wish someone would tell me how I can get out of this darned automobile!" [4] One simple design change had stymied the master.

These three examples demonstrate that even people who have built their reputations on doing things differently often make faulty or irrational decisions when moving out of the security of their comfort zones. And as Ralston, Wright, and Houdini demonstrate, it has nothing to do with courage, IQ, talent, or success.

What's Your Cyber Comfort Zone?

Scott Scheferman is a hacker turned Director of Consulting for Cylance, a cybersecurity consulting firm incorporating artificial intelligence. In a popular blog post titled *Ransomware Predictions Past, Present, Future,* he wrote: "As individuals and as a collective society, we are basically novices when it comes to understanding cyber risks, being able to identify an attack, and preparing ourselves for a compromise." [5]

This observation doesn't dismiss the value of cyber talent or years in the field. Rather, it reminds us that in cybersecurity, the number of unknowns is significantly higher than the knowns, regardless of experience and expertise.

Verizon's *2016 Data Breach Investigations Report* provides a powerful metaphor for battling these unknowns. The report asks you to imagine that a "soldier is told to guard a certain hill and keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike." [6] This metaphor plays out every day in the corporate world. Millions of dollars are invested in protecting against illegal entry into an organization's server,

yet the real threat may turn out to be a trusted employee. The scenario goes like this. Hackers identify an employee as a target and exploit that employee's vulnerability with malware or code, giving the hacker access to the C: drive or PC. The data at risk is then encrypted and becomes ransomware. If the company wants that data back, they must pay for it. In other words, the hackers, through phishing or social media, trick the employee into clicking a link and letting ransomware bypass every one of those expensive server protections. In cybersecurity, you constantly confront daily unknowns and rarely know what tomorrow may bring.

Moving out of your comfort zone requires a level of openness to considering new ideas and solutions rather than reverting to old, comfortable ways of doing things. For example, today's military leaders, more comfortable fighting tactical battles on the ground, face tough decisions because they are engaging in unfamiliar battles taking place only in space and time.

People who have built their reputations on doing things differently often make faulty or irrational decisions when moving out of the security of their comfort zones.

So how do you see things for what they are or are not when the cyber battlefield is constantly shifting in time and space with an enemy that is often invisible? How do you fight when there are no rules to follow because what happened in the past has no definitive relationship to what will happen in the future?

Answers begin with taking a contrarian viewpoint: making an assumption is neither good nor bad because within every decision lies an assumption.

Leveraging Your Assumptions for Better Decision-Making

The late Chris Argyris, management guru, father of "organizational learning," and professor at Harvard Business School,[7] illuminated the "invisible process" that formulates our thoughts leading to decisions. He created a mind map illustrating how we think called the Ladder of Inference.[8] Look at the diagram in Figure 1, and you will see that our thought process is like a ladder—each rung has a purpose.

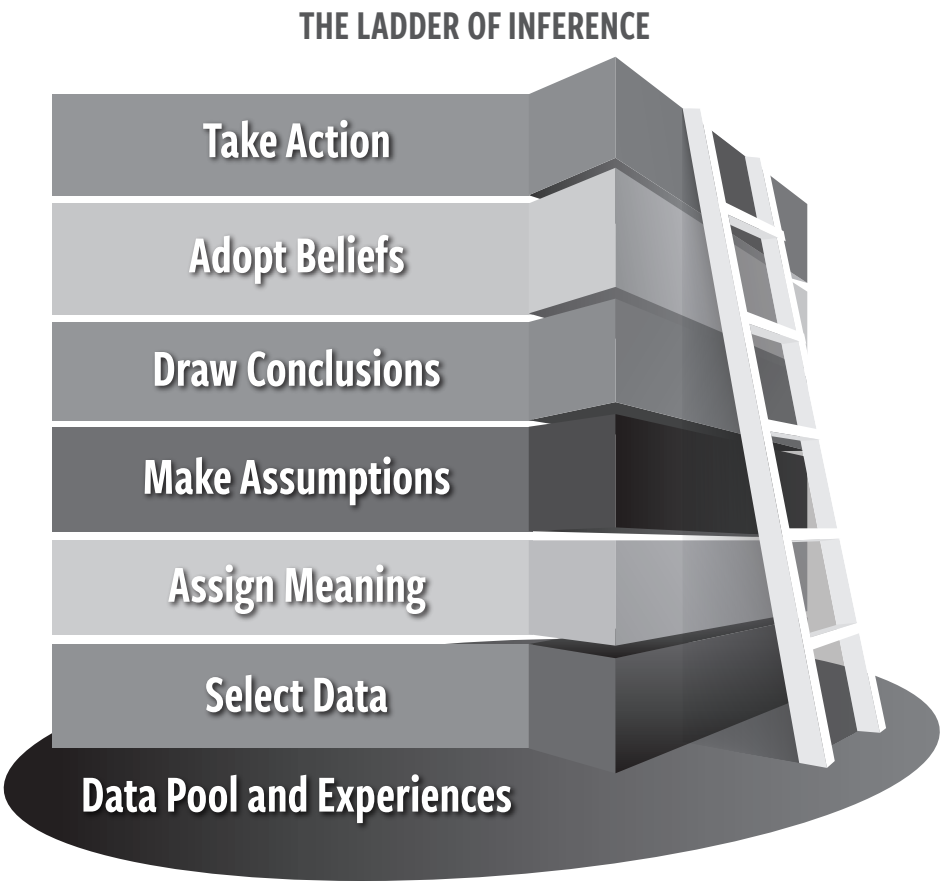


Figure 1. The Ladder of Inference. A mind map created by the late Chris Argyris.

You begin by collecting data, then sorting through that data to form your assumptions. From there, you draw an inference, making a decision that leads you to an action. It's a simple and linear process that explains much about our behavior. This is why the Ladder of Inference is so highly respected in the field of learning and development as an instructive metaphor to explain the decision-making process influencing your actions. The Ladder serves multiple purposes by helping you become more aware of your thinking, making that thinking visible and providing a way to probe what others are thinking. Understanding your "true thoughts" leads to smarter decisions. This does not diminish the value of trusting your "gut." However, there are too many decisions to make in the course of just one day, and trusting your instincts alone isn't enough to help you manage these decisions.

The Ladder illustrates that the middle rung of every decision is the assumption. The assumption is something you treat as a truth rather than simply believe; it is something taken for granted, often subconsciously.

In working with the U.S. Army, I discovered that unlike most organizations, the military very specifically addresses the assumption's role in the decision-making process. Its definition of assumption is "a supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action."[9] At the same time, I observed that the process of identifying and then challenging assumptions is not always personally internalized. As one military leader confided, "Most [in the military] recognize the importance of assumptions but don't often invest enough time in developing them."

The reason to make this "investment" is that the assumption is one of the key components behind every action. The meaning of this is significant—that is, making an assumption is as natural as breathing. To judge yourself for making an assumption is unproductive: don't be held back by blaming yourself for an action that is a natural part of the decision-making process. Instead, accept that you make assumptions by surfacing them and owning them without guilt. The process of doing this is called *making an Assumpt!,* and we will explore this process in greater detail further on. What is important to note right now is that once you make an Assumpt!, you have the power to decide if you want to invest in that assumption or challenge it.

Managing Your Assumptions Outside of Your Comfort Zone

Moving out of your comfort zone produces anxiety—approving a cyber budget might elicit the fear of failure; learning to think like the enemy might force you to consider the inconceivable; changing the way you command a team that operates better without directive leadership may drive you crazy; facing a ransomware experience may generate sheer panic as you lose everything unless you pay.

Learning to think like the enemy might force you to consider the inconceivable.

Regardless of the situation, Figure 2 suggests that there are also a number of assumptions generated when moving out of your comfort zone. These assumptions are quickly propagated for a number of reasons: fear, change, facing a new experience or confronting the inconceivable. Many of these assumptions serve the purpose of gently coaxing you back into your comfort zone as a way to reduce that anxiety. In other words, they act as barriers to new thinking or solutions. They are *dangerous.*

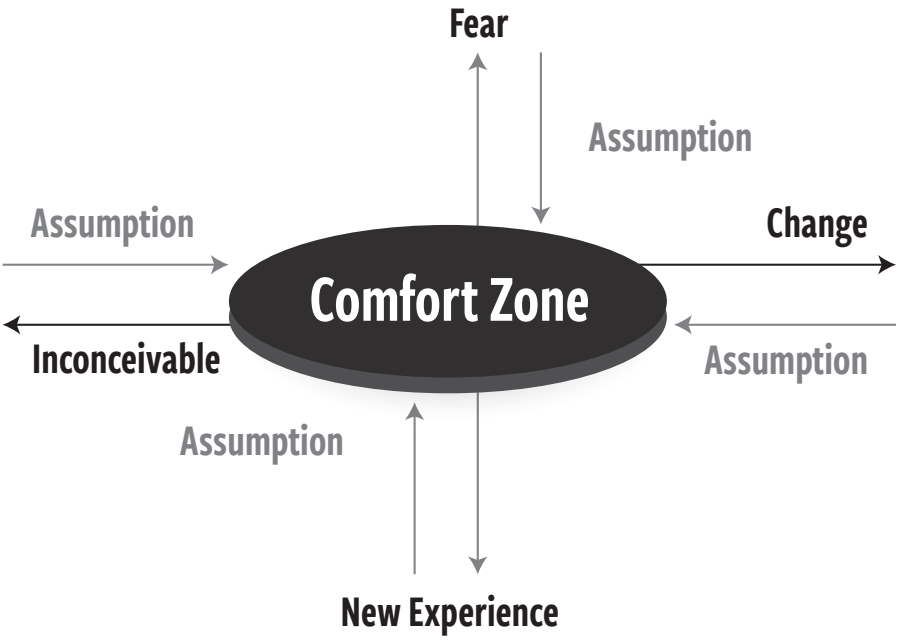


Figure 2. Assumptions push you back into your comfort zone.

For example, Micah Zenko's comprehensive book *Red Team: How to Succeed by Thinking Like the Enemy* provides a structured process that "seek[s] to better understand the interests, intentions, and capabilities of institutions or potential competitors" through "simulations, vulnerability probes, and alternative analyses." [10] The author points out that often leaders undermine the red team's goal. They fear that the exercise may uncover a leadership weakness (which is part of the purpose of the exercise) that will reflect on them (which it will). When presented with a red team proposal, a leader may point out that a red team exercise was tried a year before without results. This is a dangerous assumption to invest in on face value. Last year, a number of things could have gone wrong such as the structure not being properly set up. Or it may have gone right, and the red team didn't find any issues. The point is, what worked or didn't work last year is, on the surface, no yardstick of future success. "It didn't work last year" is a cue that an assumption is being played out as a reaction to change.

"It worked last year, so let's do it again" is also a verbal cue that an assumption is being made. In the late 1700s, a trusted Dutch military strategy for defending against the French was to flood low-lying areas, separating them from the invaders. This unique system, called *waterlinie,* had proved an effective defense for over two hundred years and through multiple wars. The Dutch *waterlinie* was designed to be deep enough to prevent walking through yet shallow enough to inhibit boating. In 1794 and 1795, however, the weather was extremely cold, and the water froze over, giving the advantage to the French who crossed the ice and won the battle. [11]

"Preparing for the last war" assumes that what worked before will work again, and the phrase serves as a strong reminder of the value in surfacing key assumptions.

A good question to ask at this point is, "How do you recognize most assumptions if they are made subconsciously?" There is no one answer to this question, but a fast solution, as mentioned before, is to listen to what you and others are saying in response to thinking differently and making a change.

You can often recognize these assumptions via verbal cues as in Figure 3.

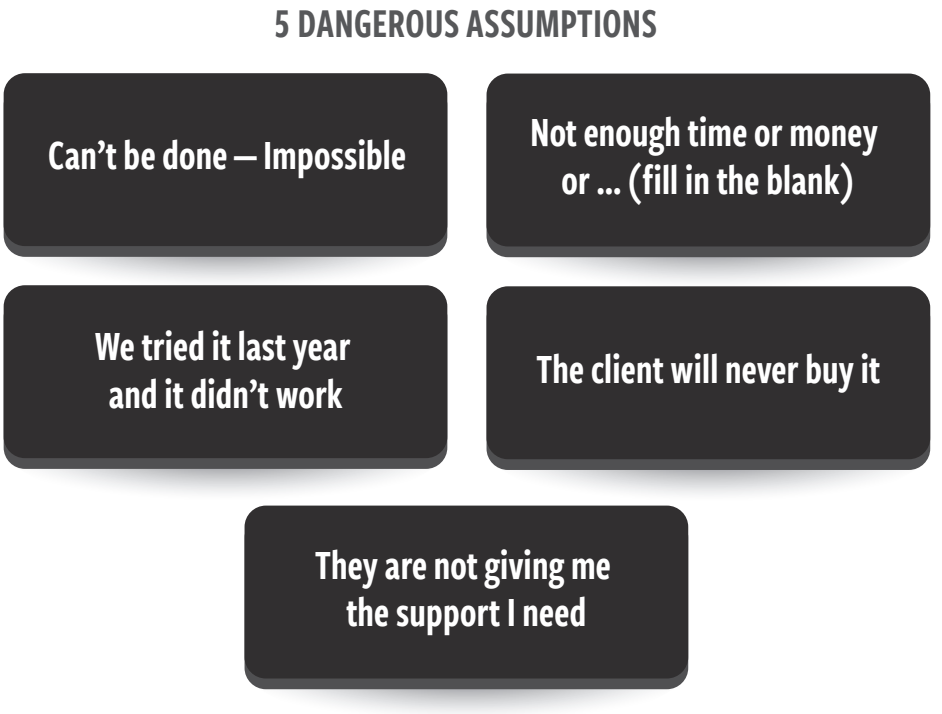


Figure 3. Verbal cues to unlock dangerous assumptions.

Over time I have collected a number of these verbal cues from all walks of business and put them into a database called the Dangerous Assumptions Database (DAD). The DAD's nomenclature pays homage to a famous leadership quote that "assumptions are the MOTHER of all screw-ups." The DAD help you identify these MOTHERS and then quickly identify certain beliefs that we treat as truths.

These include:

- "I'd never do it that way." (Thinking that the world thinks like you)
- "We are smarter than our enemy." (Believing that you and your team are the best)
- "This is good code." (Wanting to believe that the source code run through the compiler translates without flaws)
- "No one would ever do that." (Thinking that if you can't imagine doing something, others won't imagine doing it as well)

I have been collecting dangerous assumptions for years and am happy to share part of this database if you follow up with me at andy@andycohen.com. Once you enhance your ability to "listen" for assumptions, the next step is deciding how to manage them when out of your comfort zone. Let's look at an example in weapons building.

Building a Weapon Outside the Comfort Zone

General Mark A. Milley, four-star general and 39TH Chief of Staff of the U.S. Army, has been providing a wake-up call that encourages the Army to move out of its comfort zone and rethink how future wars will be fought and won. "Rapid change has become increasingly compressed," he said in a speech at the 2016 Association of the U.S. Army Annual Meeting and Exposition's Eisenhower Luncheon. "Those of us today will find it difficult to recognize the battlefield of 2035, let alone 2050 ... Crisis will unfold rapidly, compressing decision cycles and response times. Ambiguous actors, intense information wars, and cutting-edge technology will confuse situational understanding." [12]

This means the Soldier on the ground may often be operating solo, cut off from any form of communications with headquarters and peers, and must never stay in the same place past an hour or two in order to escape detection. General Milley describes a scenario in which the independent Soldier will have the ability to replace a weapon part on demand via a portable 3D printer. [13]

In light of these changes, General Milley also questions today's process to acquire and build future weapons. He suggests that the Army revisit the process, streamlining the timeline to address changing technology and the critical need for speed. [14]

Creating Cyber Weapons

Major James Twist is a lead analyst at the Army Cyber Institute at West Point and picks up on General Milley's message. In his lectures, he often shows a DoD acquisition and technology flowchart to demonstrate the complexity of acquiring a new weapon, such as a rifle, onto the battlefield. Figure 4 represents just a small portion of the chart yet clearly illustrates the number of levels, steps, and processes involved in integrating a weapon into the military.

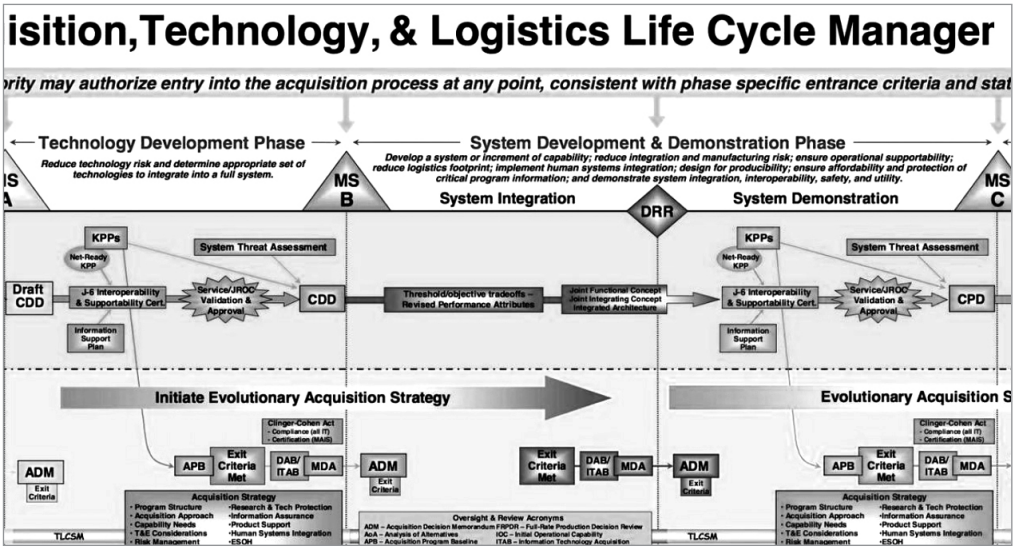


Figure 4. A portion of the DoD acquisition and technology flowchart. [15]

The challenge of working within this flowchart is that by the time the new technology (code, piece of software, digital listening device, new gear, etc.) gets processed and approved, the technology involved is already outdated.

A small team at General Motors (GM) faced a similar challenge when tasked with creating a telemetric system for future cars called *OnStar.* Nick Pudar, now Director of Strategic Initiatives at GM, tells the story of when he joined the *OnStar* team:

> In the early nineties, Rick Wagoner, then the president of GM North America, believed that the future of the auto industry went beyond fast, efficiently run, and comfortable cars and chose an *effect:* developing a new type of communications system for the car. The overall obstacles in launching this kind of product were significant. At the time *OnStar* was conceived, the typical total life cycle of a vehicle program was eight to ten years. It took two years to create the product, two years to test and integrate it into the manufacturing processes, and then four to six years of having the hardware built into the vehicles as part of the regular production run. Heavily integrated technologies such as the electronics represented by *OnStar* traditionally would need to wait many years for the next major redesign of the total vehicle. Only then would you see opportunities to implement major improvements. In contrast, the average electronic product development cycle, like *OnStar* technology, was eighteen months. It was initially assumed that these two product cycles were incompatible. [16]

So the first thing GM had to do was move out of its comfort zone by acknowledging this assumption and assessing if it was true or just a set of beliefs. Even Chet Huber, who was there in the beginning and became president of *OnStar,* said that it would have been easy to walk away from the project. Nobody really wanted to challenge the assumption of the accepted production practice.

Preparing for the last war assumes that what worked before will work again, and the phrase serves as a strong reminder of the value in surfacing key assumptions.

"Luckily, someone did," said Pudar. "Rick Wagoner empowered the team to 'follow the other hand' [by challenging their assumptions]." This allowed the team to "simply break all the product development rules, and through diligent engineering, study and identify the absolute latest integration point in the existing processes." [17] In essence, the team rejected the assumption that they had to fit an eighteen-month electronic product development cycle with an eight-year vehicle development cycle and focused on the opposite—fitting a lengthy production cycle into a shorter technology cycle.

That was in 1997. *OnStar* continued to test this assumption; within five years of the launch, they had instituted eight generations of technology updates. [18] Less than twenty years later, *OnStar* reported a subscriber base of over 7 million with more than 1 billion interactions. [19]

The willingness of GM to move out of its design and production comfort zone and challenge traditional assumptions proved beneficial in building a new business and staying ahead of the competition. The story illustrates that the Army needs to move out of its comfort zone and consider building a cyber weapon acquisition process centered on the technology rather than the other way around.

The Dark Web's Role in Cybersecurity

Once you give yourself permission to identify your assumptions, you open the door to a journey that takes you down multiple paths, leading to new opportunities and solutions. For example, rather than spend hours trying to streamline the process to acquire valuable data to use as a weapon, why not create a new channel? Instead of spending two months outsourcing the creation of an expensive code, go directly to the Dark Web. The Dark Web is considered an anonymous cyberspace where at least half of its visitors are selling illegal information, data, codes, drugs, pornography, and weapons.

Military leaders may dismiss the concept of purchasing illegal data as a nonnegotiable as it conflicts with the Army's moral code. This author can only suggest that "buying on the Dark Web" is an assumption to be recognized and then explored, rather than accepted. Major Twist suggests testing the viability of purchasing Dark Web data in order to explore the pluses and negatives as a cyber strategy for acquiring key information. [20]

Many key cybersecurity decisions are based on a risk/reward basis. For some companies, it's financially prudent to pay for the cost of an attack rather than invest unknown dollars in preventing one. What undermines the risk/reward ratio is the assumption of understanding the price of data. How much is a personal social security number or credit card actually worth to an illegal buyer? How much money will an attacker ask for to release a piece of ransomware? This information is important when determining a risk-to-reward cybersecurity strategy to protect data vulnerabilities. You might assume a specific piece of information is worth 75 cents when on the Dark Web it could sell for $1.25 or 25 cents. Either way, you are operating under a giant assumption around value instead of validating it in a real Dark Web setting where this data is sold or through insurance companies, like CyberPolicy.com, which protect against cyberattacks.

Discussions challenging accepted assumptions raise other important issues as well. For example, the Army is committed to recruiting top talent in cybersecurity. This means having to consider a software engineer who might have used drugs. Presently, this is unacceptable under Army requirement guidelines. But to see this as a *rule forever* rather than a present operative assumption hinders the discussion of how to build the best cyber team for the Army.

The Value in Thinking Like the Enemy

In the movie *Star Trek II: The Wrath of Khan* (1982), Captain James T. Kirk, played by William Shatner, reveals his character when he faces a Kobayashi Maru scenario in the form of a computer simulation where the commander of the ship can never win. The simulation occurs when he is a young cadet and ordered to save a stranded spaceship disabled in enemy territory. But that's where the no-win scenario unfolds: it's actually a trap. So saving the ship means the destruction of his spacecraft, but choosing not to mount the rescue mission will result in the destruction of the stranded spaceship.

Captain Kirk, however, beats the program by hacking into the system and rewriting the program before he faces the simulation, thus ensuring he will win. [21] In a much later release, *Star Trek* (2009), Kirk, played by Chris Pine, is initially accused of "cheating" but is later awarded a special citation by the Starfleet Academy for "thinking differently" about confronting the overall challenge. [22]

It's easy to assume that a fictitious concept has little relevance for today's cyber issues. James L. Caroland, an adjunct associate professor in the University of Maryland University

College's Cybersecurity Program, and retired Colonel Gregory Conti, former director of the Army Cyber Institute and associate professor in the United States Military Academy's Department of Electrical Engineering and Computer Science, would argue differently.

The pair performed a fascinating experiment designed to help students of cybersecurity think differently by giving them a seemingly "impossible" task.[23] Students needed to solve a problem that required memorization but whose answer could not be memorized. The only solution was to cheat, and their grade was dependent on their level of creativity in finding a way to do so. Put another way; students faced their own Kobayashi Maru: they had to cheat to pass the test.

The Army needs to move out of its comfort zone and consider building a cyber acquisition process centered on the technology rather than the other way around.

But the teachers had another catch: if students got caught cheating, they would fail. Students' solutions were both amusing and impressive. One student used his Mandarin Chinese skills to hide the answers. Another put the answer on a soda can, which could be turned away from the proctor as he walked by. The winning student used a false book cover in which the answer was coded on the back cover.

The premise behind this exercise was that "cheating will challenge students' assumptions about security and the trust models they envision."[24] According to the professors of the course, it is through "learning the thought processes of our adversaries that we can hope to unleash the creative thinking needed to build the best secure systems, become effective at red teaming and penetration testing, defend against attacks, and conduct ethical hacking activities."[25]

The purpose of this research was to help these students become more responsible in this field. According to the professors, "By anticipating such actions and reactions, ethical actors are far better prepared to build secure systems and perform both defensive and offensive activities successfully."[26]

In short, thinking like the enemy helps you defeat the enemy. Thinking like your competition helps you win against them. Thinking like your boss helps you understand him or her. Thinking like your peers helps you ensure alignment with them.

In the case of cyber espionage, thinking like the adversary doesn't mean you have to act like one. But not thinking like the adversary is cheating yourself from being one step ahead of the enemy. And that is a terrible cybercrime.

The Assumpt! Strategy in Cybersecurity

The goal of the Assumpt! is to raise individual and organizational consciousness in identifying key assumptions and converting them to truth assumptions in order to make faster, smarter decisions. A truth assumption is one that has been surfaced, explored, and tested.

Making an Assumpt! is the act of acknowledging to yourself and others that an assumption is being made while reserving judgment about the specific nature of that Assumpt! Try this. The next time you meet someone for the first time, try to recognize the immediate assumptions you make and turn them into Assumpts! The list is endless but may include, "My Assumpt! is that he or she is successful/is a jerk/has a weak handshake/is a lousy dresser/must be really smart/can't be too bright/isn't very dynamic ..." Then, before acting on that Assumpt!, decide what you want to do with it.

The goal of the Assumpt! is to identify key assumptions and convert them to truth assumptions in order to make faster, smarter decisions.

Acknowledging your assumptions opens the door for you to examine your beliefs before acting on them and encourages others to challenge them. This might seem contrary to the directive leadership that kinetic combat often requires, as leaders are expected to "know" to give orders. There are times when this kind of decisiveness is necessary, but at other times, acknowledging your Assumpts! makes for a stronger leader. The following are sample cybersecurity Assumpts! to consider challenging.

Case A: A board of directors received a cybersecurity agenda. One of the points was, "Are we doing enough?" This is a common question that many leaders in both the military and non-military ask. But in cybersecurity, *doing enough* assumes the same quantifiable parameters as "Do we have enough insurance?" "Did we budget enough for salaries?" or "Have we spent enough time analyzing the information?" These are good questions, but the assumption is that cyber is finite. It's the difference between looking at the universe that has a beginning and end versus considering the universe as infinite and then reconciling what that means.

Perhaps "Are we doing enough?" could be replaced with "How do we sustain our cybersecurity efforts?" or "What is our strategy for adapting to cybersecurity attacks that constantly change over time?" Acknowledging *enough* as an Assumpt! gives you the ability to shift perspectives and provides new pathways to the solutions you seek.

Case B: The military, like most organizations, believes itself superior to the competition. In cybersecurity, how do you define *superior*? If superiority can be measured by results, then you must assume that you are either winning or losing the war. But in cybersecurity, are you fighting small battles or one big war? If you are willing to see *superiority* as an Assumpt!, then it opens the door that "whatever we do, someone else can do." And rather than assume that is a weakness, see it as a strength because it assures your role on the offense, never underestimating the power of your attacker.

The Assumpt! as an Antidote to Moving Out of Your Comfort Zone

The four steps below outline the Assumpt! flow.

1. **Expand:** Ditch the bias that assumptions are "something I shouldn't make." Accept, without judgment, that assumptions are part of your ladder of thinking and decision-making processes. Within every decision lies an assumption.
2. **Identify:** Listen to the verbal cues generated when moving out of your comfort zone. Be aware of how your present emotional state influences those assumptions. Bring them to the surface. The act of identifying an assumption is called making an Assumpt! Assumpt! is a term coined to help people separate the concept of an assumption from actually making one.
3. **Accept:** Accepting your Assumpts! means acknowledging that you can live with the consequences of where your Assumpt! leads you (i.e., you can leave your Assumpt! "unchecked"). This is an important point as many assumptions are beneficial and serve to help you make decisions quickly and accurately.
4. **Challenge:** This step is when you decide to *check* your Assumpt! My Assumpt! is this is what General Milley was suggesting when he said, "Every assumption we hold, every claim, every assertion, every single one of them must be challenged." [27] There are three levels in the challenge.

    a. **Question:** Questioning this Assumpt! may be as simple as stating, "Perhaps if I tried to do this in a different way ..."

    b. **Explore:** The next level is to explore the Assumpt! in detail to determine the origin of the idea: "What is the Assumpt! based on, and what are the consequences in accepting it?"

    c. **Reject:** The fastest way to create new thinking is to reject your Assumpt! This is what GM did when saying that the production cycle had to adapt to the technology cycle rather than the other way around.

There are more steps to take in identifying and challenging your Assumpts! than outlined in this paper. The main point is that in cybersecurity, we are all learning. And when it comes to moving out of your comfort zone, talent, IQ, and experience don't often matter. Success in conducting business or warfare in unchartered territories is dependent on how you identify and manage the assumptions generated in dealing with the movement away from your comfort zone that drive (in) security.

And it is this author's Assumpt! that this process can change your approach to cybersecurity in as little as one assumption at a time.

NOTES

1. Rick Maze, "Radical Change Is Coming: Gen. Mark A. Milley Not Talking About Just Tinkering Around the Edges," Association of the United States Army, December 13, 2016, https://www.ausa.org/articles/radical-change-coming-gen-mark-milley-not-talking-about-just-tinkering-around-edges.

2. Aron Ralston, interview, *Today*, June 4, 2003 (prerecorded), http://www.nbcuniversalarchives.com/nbcuni/clip/51115075415_s22.do.

3. David McCullough, *The Wright Brothers* (Simon & Schuster, 2015).

4. Thomas J. Shimeld, "Harry Houdini's Final Escape," Chapter 5 in *Walter B. Gibson and The Shadow* (McFarland & Company, 2005), 52.

5. Scott Scheferman, "Ransomware Predictions Past, Present, Future," *ITSP Magazine,* July 7, 2016, https://itspmagazine.com/from-the-newsroom/ransomware-predictions-past-present-future-past.

6. Verizon, *2016 Data Breach Investigations Report* (Verizon, 2016), 6.

7. Jill Anderson, "Remembering Professor Chris Argyris," Harvard Graduate School of Education, November 22, 2013, http://www.gse.harvard.edu/news/13/11/remembering-professor-chris-argyris.

8. Peter M. Senge et al., *The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organization* (Crown Business, 1994), 243.

9. *Department of Defense Dictionary of Military and Associated Terms,* November 8, 2010 (last amended February 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

10. Amazon description of Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy* (Basic Books, 2015), https://www.amazon.com/Red-Team-Succeed-Thinking-Enemy/dp/0465048943.

11. Peter Rus LION, "The Illusion of Being in Control—Part 1," LinkedIn, October 5, 2016, https://www.linkedin.com/pulse/illusion-being-control-part-1-peter-rus; Gerard Koot, "The Water Fortifications of the Dutch Republic," 2014, http://www1.umassd.edu/euro/resources/imagesessays/waterfortificationsofthedutchrepublic.pdf.

12. C. Todd Lopez, "Milley: Army on Cusp of Profound, Fundamental Change," U.S. Army, October 6, 2016, https://www.army.mil/article/176231/milley_army_on_cusp_of_profound_fundamental_change.

13. Ibid.

14. Matthew Cox, "Army Chief Wants Power to Select New Pistol," Military.com, March 10, 2016, http://www.military.com/daily-news/2016/03/10/army-chief-wants-power-to-select-new-pistol.html.

15. Noah Shachtman, "Pentagon's Craziest PowerPoint Slide Revealed," *WIRED,* September 13, 2010, https://www.wired.com/2010/09/revealed-pentagons-craziest-powerpoint-slide-ever/.

16. Andy Cohen, *Follow the Other Hand: A Remarkable Fable That Will Energize Your Business, Profits, and Life* (St. Martin's Press, 2006).

17. Ibid.

18. Ibid.

19. Stefan Cross, "OnStar Tops 1 Billion Customer Interactions," July 29, 2015, http://media.chevrolet.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2015/jul/0729_onstar.html.

20. Much of the information in this section taken from author's personal interviews with Major Jim Twist, October 5 and 25, 2016.

21. *Star Trek II: The Wrath of Khan,* directed by Nicholas Meyer (1982).

22. *Star Trek,* directed by J. J. Abrams (2009).

23. Gregory Conti and James Caroland, "Embracing the Kobayashi Maru: Why You Should Teach Your Students to Cheat," *IEEE Security and Privacy* 9, no. 4 (July/August 2011): 48–51, doi:10.1109/MSP.2011.80.

24. Ibid.

25. Ibid.

26. Ibid.

27. Rick Maze, "Radical Change Is Coming: Gen. Mark A. Milley Not Talking About Just Tinkering Around the Edges," Association of the United States Army, December 13, 2016, https://www.ausa.org/articles/radical-change-coming-gen-mark-milley-not-talking-about-just-tinkering-around-edges.