# In an evaporating OODA loop, time is of the essence

By **Jan Kallberg**

Jul 28, 2020

Both the accelerated execution of cyberattacks and an increased ability to, at machine speed, identify vulnerabilities for exploitation compress the time window that cybersecurity management has to address unfolding events. In reality, we assume there will be time to lead, assess and analyze, but that window might be closing rapidly. It is time to face the issue of accelerated cyber engagements.

If there is limited time to lead, how do you ensure that you can execute a defensive strategy? How do we launch countermeasures at speed beyond human ability and comprehension? If you don't have time to lead, the alternative would be to pre-authorize.

---

In the early days of the Cold War, planners and strategists who were used to having days to react to events faced the threat of intercontinental ballistic missiles that forced decisions within minutes. The solution? Pre-

authorization. The analogy between how the nuclear threat was addressed and cybersecurity works to a degree, but we have to recognize that the number of possible scenarios in cybersecurity could be in the hundreds, and we need to prioritize.

The cybersecurity pre-authorization process would require an understanding of likely scenarios and the unfolding events to follow these scenarios. The weaknesses in pre-authorization are several. First, there are limitations on the scenarios that we create because these scenarios are built on how we perceive our system environment. This is exemplified by the old saying: "What gets us into trouble is not what we don't know. It's what we know for sure that just ain't true."

The creation of scenarios as a foundation for pre-authorization will be laden with biases, the assumption that some areas are secure when they in fact are not, and the inability to see attack vectors that an attacker sees. So the major challenge becomes when to consider pre-authorization and to create scenarios that are representative of potential outfalls.

---

One way is to look at the different attack strategies used earlier. This limits the scenarios to what has already happened to others but could be a base to which additional scenarios are added. As we progress, artificial intelligence becomes an integrated part of offloading decision-making, but we are not there yet. In the near future, artificial intelligence can cover parts of the managerial spectrum, increasing the human ability to act in very brief time windows.

The second weakness is the pre-authorization's vulnerability against probes and reverse engineering. Cybersecurity is active 24/7/365 with numerous engagements on an ongoing basis. Over time, by using machine learning, automated attack mechanisms can learn how to avoid triggering pre-authorized responses by probing and reverse-engineering solutions that will trespass the pre-authorized controls.

So there is no easy road forward, but instead a tricky path that requires clear objectives, alignment with risk management and an acceptance that the final approach to address the increased velocity in the attacks might not be perfect. The alternative — to not address the accelerated execution of attacks — is not a viable option. That would hand over the initiative to the attacker and expose the organization for uncontrolled risks.

Repeatedly through the last two years, I have read references to the "observe, orient, decide, act" loop and the utility of the OODA concept for cybersecurity. The OODA loop resurfaces in cybersecurity and information security managerial approaches as a structured way to address unfolding events. The concept of the OODA loop, developed by John Boyd in the 1960s, centers around observing the events unfolding, orienting your assets at hand to address the events, making up your mind of what is a feasible approach and then acting.



The OODA loop has become been a central concept in cybersecurity the last decade, as it is seen as a vehicle to address what attackers do by deciding when, where and what you should do and how to do so most effectively; essentially, you need to get inside the attacker's OODA loop to understand the adversary and tailor your own defensive actions.

Retired Army Col. Tom Cook, former research director for the Army Cyber Institute at West Point, and I wrote in 2017 an IEEE article titled "The Unfitness of Traditional Military Thinking in Cyber," in which we questioned the validity of using the OODA loop in cyber when events are going to unfold faster and faster. Today, in 2020, the validity of the OODA loop in cybersecurity is on the brink to evaporate due to increased attack speeds. The time needed to observe and assess, direct resources, make decisions, and take action will be too long to be able to muster a successful cyber defense.

Attacks occurring at computational speed worsens the inability to assess and act, and the increasingly shortened time frames likely to be found in future cyber conflicts will disallow any significant, timely human deliberation.

I have no intention of being a narrative impossibilist, who presents challenges with no solutions, so the current way forward is pre-authorizations. In the near future, the human ability to play an active role in rapid engagement will be supported by artificial intelligence decision-making that executes the tactical movements. The human mind is still in charge of the operational decisions for several reasons — control, larger picture, strategic implementation and intent. For cybersecurity, it is pivotal for the next decade to be able to operate with a decreasing time window to act.

*Jan Kallberg is a research scientist at the Army Cyber Institute at West Point, the managing editor for the Cyber Defense Review and an assistant professor at the U.S. Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy or the U.S. Defense Department.*

Share:

›