Daniel E. Geer Jr.
In-Q-Tel

Children of the Magenta

The term "children of the magenta" traces to 1997, when American Airlines captain Warren Vanderburgh said the industry has made pilots too dependent on monitoring the magenta lines on the machines that are really flying the plane (http://99percentinvisible.org/episode/children-of-the-magenta-automation-paradox-pt-1).

William Langewiesche's article analyzing the June 2009 crash of Air France flight 447 comes to this conclusion: "We are locked into a spiral in which poor human performance begets automation, which worsens human performance, which begets increasing automation" (www.vanityfair.com/news/business/2014/10/air-france-flight-447-crash).

University of Miami professor Earl Wiener proposed a set of "laws" that include every device creates its own opportunity for human error; exotic devices create exotic problems; and digital devices tune out small errors while creating opportunities for large errors.

Langewiesche's rewording of these laws is that "the effect of automation is to reduce the cockpit workload when the workload is low and to increase it when the workload is high" and that "once you put pilots on automation, their manual abilities degrade and their flight-path awareness is dulled: flying becomes a monitoring task, an abstraction on a screen, a mind-numbing wait for the next hotel."

Nadine Sarter of University of Michigan said that such "de-skilling is particularly acute among long-haul pilots with high seniority." As Langewiesche added, "Beyond the degradation of basic skills of people who may once have been competent pilots, the fourth-generation jets have enabled people who probably never had the skills to begin with and should not have been in the cockpit."

The situation in aviation is precisely the situation we are in with cybersecurity. Human error is rampant at all levels. There is a cacophony of calls for cybersecurity automation. The most experienced people are no longer directly solving problems hour after hour but rather superintending largely automated processes. More and more, digital devices tune out small failures, whether they be attacks, misconfigurations, version mismatches, or service disconnects. Like airplanes automated enough that anyone can fly them, anyone can ostensibly operate the digital devices that are unarguably society's predominant risk vector. Therefore, there's a guarantee of large errors at some future point—errors that no one still in practice will handle. When successful automation makes particular threats increasingly unlikely to appear, the interval between failure events grows longer. As the latency between failure events grows, the assumption that safety has been achieved also grows, fueling increased dependence on what is now a positive feedback loop (http://geer.tinho.net/geer.sfi.2x14.txt).

Vanderburgh's "children of the magenta" also applies to cybersecurity in another way: you shouldn't run a cybersecurity detection and response operation via on-the-fly reprogramming of our equivalent of the Flight Management Computer. In 2013, *Aviation Week* editorialized that "there needs to be a new performance-based model that requires flight crews to log a minimum number of hand-flown takeoffs and departures, approaches and landings every six months, including some without autothrottles. Honing basic pilot skills is more critical to improving airline safety than virtually any other human factor" (http://aviationweek.com/commercial-aviation/editorial-how-end-automation-dependency).

If you aren't regularly flying your cybersecurity airframe manually, you can and will become automation dependent. Then, just as with airplane pilots, in a rapidly changing environment, you'll lose situational awareness due to task saturation brought on by the automation itself. We can't allow ourselves to be so automation dependent that we can't turn off the automation and fly the plane. ■

Daniel E. Geer Jr. is the chief information security officer of In-Q-Tel. Contact him at dan@geer.org.

1540-7993/15/$31.00 © 2015 IEEE