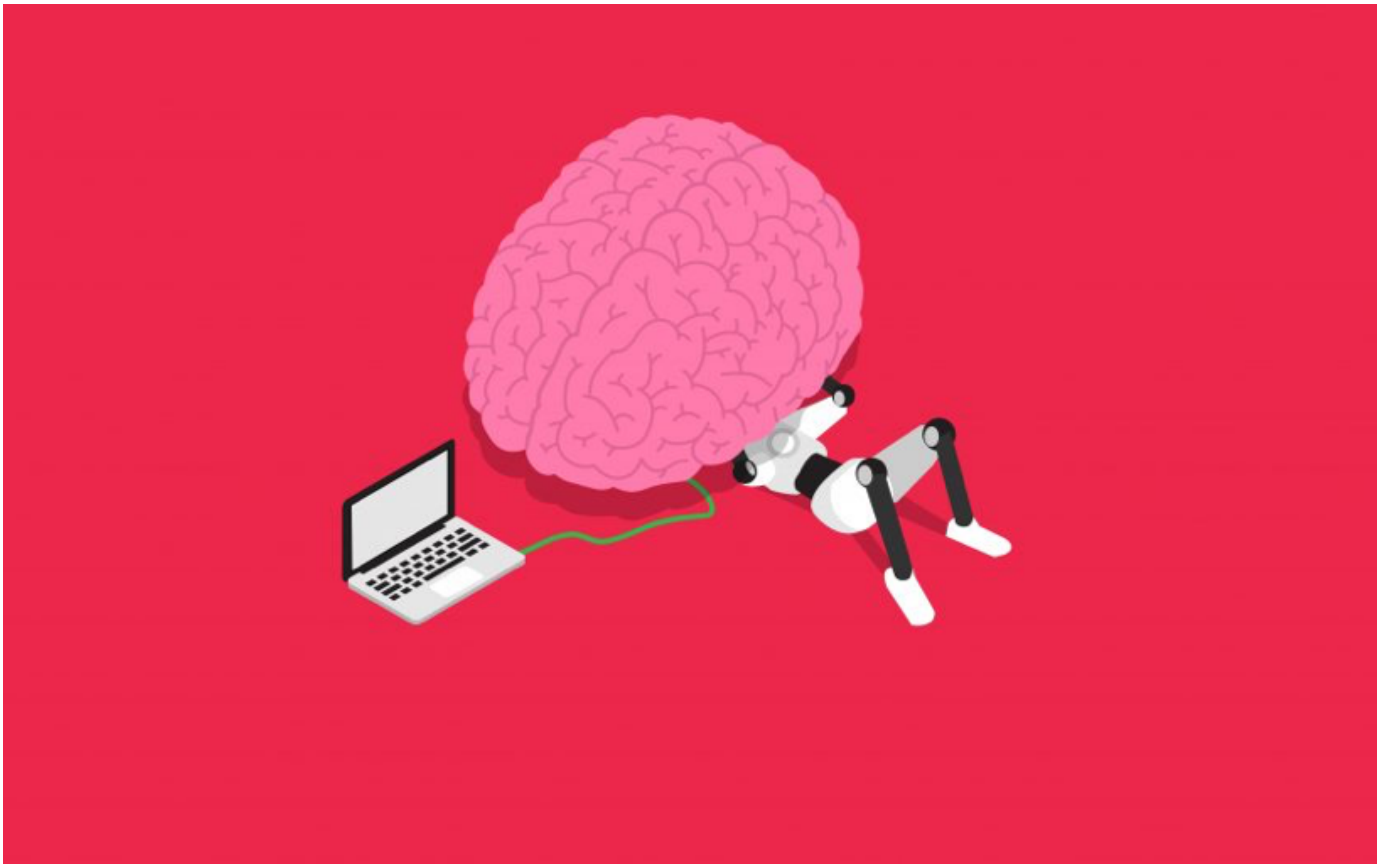
It's Time to Get Real About Artificial Intelligence

Gerd Leonhard May 14, 2019



Artificial intelligence has become a global buzz-phrase that gets massive media attention yet remains broadly misunderstood, at least in terms of what is real about so-called AI today and its potential impact on the future.

As a business leader justly concerned about the potential role of AI in cybersecurity, you can't afford to fall into the hype trap, regardless of whether it's utopian or dystopian.

First, let's state that AI is neither artificial nor intelligent (in the human sense of that word). Every machine, algorithm or technology is "artificial," i.e., not organic or biological. So this is hardly unique to AI. And true, broad intelligence in the human sense—intellectual, emotional, kinesthetic—is still a faraway goal for even the most advanced machines.

IA, not AI as in ‘Ex Machina’

Therefore, I would propose to simply use “smart machines” or “intelligence assistance” (IA) as more suitable terms.

If you buy into the much-hyped fears around AI – that machines are somehow on the verge of taking over the world – you may miss a big opportunity to use the technology to make your organization more secure and innovative.

On the other hand, if you over-inflate what AI or IA can actually do for you today, you may make your organization more vulnerable to cybersecurity threats by minimizing the importance of the human element. Dehumanization is never going to be a benefit!

To find the right balance, let’s start with three fundamental guidelines to follow in approaching AI today:

1. **Don’t let fear run your decisions—but keep asking the right questions.** We are many years away from the Hollywood worlds of robots using their superior intelligence to do away with humans. Not that such a potentiality isn’t possible or dangerous (it is—which is why I am all for regulating Artificial General Intelligence/AGI); it’s just that the technology is probably 30 to 50 years down the road. In the meantime, what I currently characterize as IA, can be an immensely powerful tool in driving business decisions and improving cybersecurity protections.
2. **When we deploy smart machines, we humans can’t get too lazy.** There is a tendency to assume that if intelligent machines are on the job, there is no need for human intervention or decision-making. This is abdication and will be quite dangerous. Humans have many qualities (I call them the androrithms) that machines don’t, particularly in examining complex decisions that require context, ambiguity, nuance, intuition, judgment, empathy, imagination and other human characteristics. An intelligent machine might do a better job than a doctor at analyzing 5 billion images of skin cancer, but

should the doctor simply accept what the machine tells her and prescribe medication without talking to the patient and examining other factors, such as the quality of the patient's life?

3. **We should not allow the use of AI to result in increasing de-humanization.** We must always remember that it is our humanity that will make all the difference in a world dominated by algorithms and smart machines. As I discuss in my book "Technology vs. Humanity" our future is to become more human, not less, and today the biggest danger is not that machines will eliminate us, but that we will become too much like them. If we as business leaders choose to fire people or subjugate people to the reductionism of binary algorithms, we are not using these technologies to their full potential. Machines are there to help people, to assist them, not to substitute them. Technology is not what we seek but how we seek!

AI in Cybersecurity Today

I stated earlier that a more accurate definition for what we call "artificial intelligence" would be "intelligent assistance." Computers are very good at binary information—limited and targeted, but infinitely scalable. They are invaluable in memorizing the facts in oncology reports or analyzing cybersecurity attack patterns. But it is difficult if not impossible for computers to do more human things, like reading body language or understanding sarcasm—simply because they lack human context and because they don't exist. As some philosophers would say, they have quanta but not qualia. Machines are binary, humans are multinary!

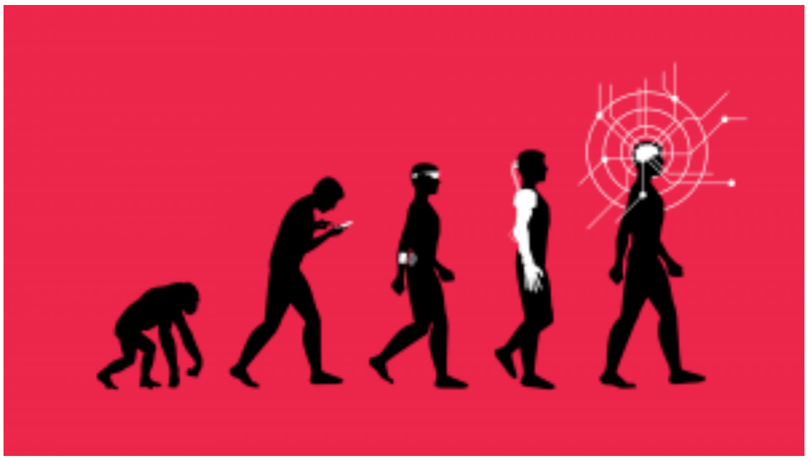
The type of intelligence and machine learning that is available in today's technology make it particularly well suited to provide intelligence assistance to the typical cybersecurity challenges that organizations face, as long we keep awesome humans in the loop.

For example, software can analyze patterns and learn from experience to recognize new and similar patterns. AI machines have the capacity to scale and examine infinitely more patterns than humans. They can tell us they've seen a certain pattern before and recommend methods to respond to both existing and new attack vectors.

They bring a computational value that humans can't match. But that doesn't mean they should replace humans. One of the paradoxes of computers is that when you have too much information that is unstructured, ambiguous and constantly changing, the machine will not be able to make a decision (the so-called intractable problem). To use them effectively, particularly in cybersecurity, we have to be careful of assuming that they are always right, and we should employ a healthy skepticism of what they are showing us.

AI's Vast Potential

Having offered those provisos in terms of where AI is today, it is hard to overstate the dramatic impact that AI technology will have on the world in the coming years, including the world of cybersecurity. In my brief film called "We Need to Talk About AI," I note that AI will be the greatest wealth generator of our time, enabling us to cure diseases, enable smart cities, redefine poverty and tackle our foremost environment challenges.



As business leaders and as citizens, we all have a rare opportunity to begin building an ethical framework for using AI technology to help humanity achieve these formidable achievements. Cybersecurity should be an important area of innovation and investment. It is also an area where digital ethics is now moving centerstage. As we look ahead and begin the path towards a world in which machines increasingly act like humans, we must avoid the trap of surrendering to the algorithm and having humans behave more like machines.

Gerd Leonhard is a leading global futurist keynote speaker and author of five books, including the best-selling "Technology vs Humanity" (2016), available in 11 languages. He has worked with many Fortune 500 companies as well as governments and NGOs. He made a short film, "We Need to Talk About AI," and has a new digital ethics newsletter: www.digitalethics.co