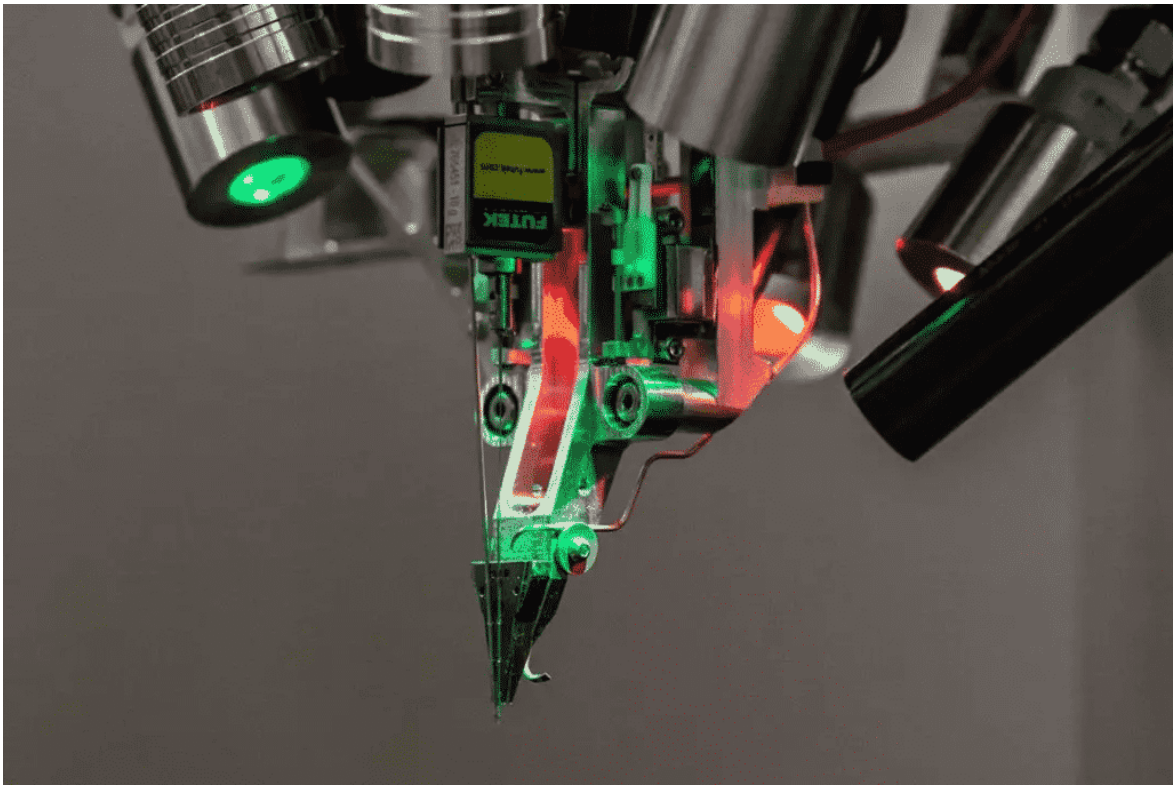

Elon Musk's Neuralink May Give AI The Keys To Our Brains

Elon Musk is a consummate Technocrat and Transhumanist who sees the merger of the human condition with advanced technology as the way to achieve Humanity 2.0. Remember that Technocracy is the "Science of Social Engineering." ▯ TN Editor

When Elon Musk gave the world a demo in August of his latest endeavor, the brain-computer interface (BCI) Neuralink, he reminded us that the lines between brain and machine are blurring quickly.

Though Neuralink and BCIs alike are still likely many years away from widespread implementation, their potential benefits and use cases are tantalizing, especially as the technology eventually evolves from stage 1 applications, such as helping those with spinal cord injuries, to more complex ones, such as controlling multiple devices.

It bears remembering, however, that Neuralink is, at its core, a

computer — and as with all computing advancements in human history, the more complex and smart computers become, the more attractive targets they become for hackers.

To be sure, the consequences of high-level hacking today are severe, but we've never before had computers linked to our brains, which seems a hacker's ultimate prey.

Our brains hold information computers don't have. A brain linked to a computer/AI such as a BCI removes that barrier to the brain, potentially allowing hackers to rush in and cause problems we can't even fathom today. Might hacking humans via BCI be the next major evolution in hacking, carried out through a dangerous combination of past hacking methods?

To better understand how hacking the brain could happen, let's first examine how the relationship between humans, computers and hacking has evolved over time.

1980s To Mid-1990s: Hacking Tech To Get Human Data

Though hacking has been around since the 1960s, the modern age started in the 1980s when personal computers — and then hackers — made their way into homes.

Hacking took advantage of new and emerging technology that was easily manipulated. Hackers' treasure during this time was mainly personal and financial information, such as credit card details, and they leveraged technology to get it.

The 1992 film *Sneakers* — about a black box capable of breaking any encryption code, ensuring there were "no more secrets" — helped popularize and reveal some of the hacking techniques used at the time, such as infiltration, physical intrusion and backdoor access. During this time, computers were the conduit to human data.

Mid-1990s To Today: Hacking Tech Via Humans

As technology became more accessible, humans began storing more of their private, sensitive information *within* technology, which now held

the keys to hackers' treasure.

While the core theme of *Sneakers* was to use a black box to cryptographically decipher systems, social engineering was heavily used to gain access to the box — a tactic that has grown exponentially as hackers shift their approach. Instead of breaking into the technology itself, hackers began preying on the vulnerabilities of human behavior (the weakest link) to get into the tech we rely on to store our vital information.

This period has been dominated by phishing and all forms of social engineering — hackers' psychological manipulation of humans to persuade them into doing the hackers' bidding. During this period, humans have been the conduit to technology.

Read full story here…