EFFICIENCY IS EASY TO HACK

As we embed Internet of Things-enabled devices through our physical world, we need to remember to secure them against cyberattacks.

BRIAN DAVID JOHNSON

Connecting an appliance to the Internet provides not only the opportunity for added functions and efficiency but also the potential for hackers to exploit security lapses.

West Point is a strategic location, a high bluff overlooking an S-shaped bend on the Hudson River. During the Revolutionary War, the army that held that spot controlled commerce and communication between Albany and New York City. In 1780, the British were willing to give Benedict Arnold a small fortune to deliver it to them.

Today, West Point is the home of the United States Military Academy. But just south of the academy, in the town of Highland Falls, is a new addition to the country's security infrastructure. The Army Cyber Institute is a think tank chartered to explore the future of cyber threats and what it will mean to the Army five to ten years in the future. It is part of a larger web of institutions and military commands across all the U.S. Armed Forces dedicated to understanding and countering the threat from cyberattacks and information warfare.

We expect the U.S. military to be a lean, mean, fighting machine, so cybersecurity may seem like an esoteric thing for it to be concerned with. But the Armed Forces are grappling with many of the same cybersecurity threats that private companies face. Indeed, part of the mandate for the

Cybersecurity experts have demonstrated that Internet-connected vehicles are vulnerable to attack by hackers.

Army Cyber Institute is to bring together military commanders and experts from private industry to discuss and assess these threats and evaluate potential countermeasures.

Last summer, I led an event that tasked a diverse group of thought leaders with envisioning future digital and physical threats. The threatcasting process we followed is a conceptual framework designed to enable multidisciplinary groups to envision and plan in a systematic fashion against threats ten years in the future. From a wide array of multidisciplinary research, groups craft possible visions for the future of digital and physical security.

The goal of event was not only to model multiple future threats, but also to imagine clear next steps that organizations could take to avoid these coming threats. The event provided a platform for thinking and discussing the future, so that all the attendees could continue to process new information and developments.

One of the key findings from the event was that the technological, cultural, and economic shifts and advances in the next decade will bring about a different threat landscape than the one we are used to. To borrow a term from military thinkers, cyber and data security represents a widening attack plain that includes more private citizens, an increasing number of targets, and ultimately a fundamental change in the very nature of security and threat.

More intriguing to me, however, is the unique vulnerability that engineers are unintentionally creating when they build artificial intelligence into highly automated systems.

Globally there is no norm or accepted practice for human oversight of those systems or how—or whether—the "human remains in or on the loop." Humans are slow, error-prone, and costly, so the more a system can operate without human oversight and input, the more potential it has to provide a level of efficiency and productivity that could prove to be disruptively profitable.

As more physical systems undergo a wave of AI-driven automation with the driving factor being efficiency, those systems become increasingly vulnerable to attack. It turns out that efficiency is easy to hack.

The Calculus of Risk

Lt. Col. Joshua Bundt is a computer scientist who has spent 16 years as an officer securing communications and computer networks for the U.S. Army. Today, he is a researcher at the Army Cyber Institute and a professor at West Point, where he teaches program analysis and digital forensics.

"When we're designing for efficiency we try to streamline specific areas like a manufacturing processes, time to market, or a better user experience," Bundt explained. "When we do this we might succeed in making these areas more efficient, but then they are not secure. Because typically systems that are secure are not efficient."

It is possible to design a simple system that is both efficient and secure, but keeping it that way is a challenge. A successful system will face pressure—from internal stakeholders or market forces—to expand. For instance, in the early 2000s industrial and medical equipment began shipping with Windows XP rather than purpose-

built operating systems. That made it easier to train new users, but even lightweight versions of a PC operating system are more complex than is absolutely necessary to run industrial equipment. And that increasing complexity creates the opportunities for vulnerabilities to creep in.

Security is an almost unwitting victim of efficiency.

"Complexity and security don't go together," Bundt continued. "It's a well-accepted fact that complexity is the enemy of security. When we try to design secure systems, the basic principles are to keep it as simple as possible. But when we introduce more and more complexity, it's harder to hold to this. It becomes almost impossible to be able to do a formal analysis and confirm that the system acts and behaves in a secure manner."

And while complex software is notoriously buggy, the problem extends to hardware as well. Over the past decade, for instance, our phones have morphed from simple voice transmitters and receivers to Internet-connected devices that form the nexus of personal and professional data networks, and payment by phone is beginning to replace cash in some places. The humble home thermostat and dimmer switch are being supplanted by smart devices that can be operated remotely, and some companies have prototype Internet-enabled refrigerators that would allow users to reorder groceries from a touchscreen panel on the door.

Those added features come at a cost. If the physical system is constructed with efficiency as its first priority, then that system is vulnerable to an individual or group that wants to disrupt, vandalize, or hijack that system. Already, hackers have compromised IoT devices ranging from fridges to toys, and security experts have shown that self-driving vehicles are open to cyberattack. The threat increases as we move into the future, since these bad actors can weaponize data and AI to heighten the intensity and efficacy of the attack.

Most systems today are designed with security as an afterthought. The shipping of an efficient product is rewarded by investors and consumers. At the moment, at least, security is not rewarded by the market, and complex digital systems accept a degree of risk as they take on more complexity or are designed solely for efficiency. If an organization's e-mail server or web application goes down, for instance, usually the organization doesn't shut down fully. Even if the organization faces a larger attack or breach of security, rarely are the consequences dire enough to change the calculus of risk.

> "IT'S A WELL-ACCEPTED FACT THAT COMPLEXITY IS THE ENEMY OF SECURITY."
>
> — Lt. Col. Joshua Bundt
> U.S. Army

As we see more connected devices make their way into our work and home lives with the IoT, smart cities, and autonomous systems, this lack of awareness of how critical these systems are will become a major vulnerability. Today, these linked systems are not designed or designated as "critical systems." As they grow in sophistication and spread throughout the physical world, these systems will become an important part of our professional, medical, and educational infrastructure.

Unfortunately, until they are treated with the same severity and precautions for redundancy and security as other similar systems, such as the energy grid or water infrastructure, our reliance on IoT and smart systems will leave us vulnerable, exposed to threats, and primed for disruption.

Exploitable Vulnerabilities

The experts brought together for the threat-casting session I held for the Army Cyber Institute were incredibly diverse: not just Army cybersecurity officers, but leaders from the New York City Police Department, Citibank, various academic institutions—even one of the creators behind Marvel Comics' *X-Men*.

During the event, we explored a number of

MOST SYSTEMS TODAY ARE DESIGNED WITH SECURITY AS AN AFTERTHOUGHT. AT THE MOMENT, AT LEAST, SECURITY IS NOT REWARDED BY THE MARKET.

potential scenarios where the interface between the cyber and physical worlds—which allow for increased efficiency when all works as designed—creates an exploitable vulnerability. One scenario involved smugglers who activated malware to swamp the express package delivery system with orders of milk from smart refrigerators, leaving replacement parts for shipping container scanners sitting in the warehouse. With those scanners left unrepaired, contraband—even weapons of mass destruction—could be smuggled in.

The power of the threatcasting process comes from the combined perspectives and the wide variety of domain expertise gathered in the room. The multiple threat futures that were modeled pulled from private industry knowledge, law enforcement experience and best practices, and academic research, as well as military tactics and training. These small teams modeled a person who experiences the threat. The details of the effects-based models then helped the broader group identify how to disrupt, mitigate or recover from the threat. It was the military perspective that gave the group a new way of looking at security and efficiency.

The military is, by design, not efficient when it comes to securing a position. When a company of soldiers is dispatched to a position, they first attempt to make it secure or at least as secure as possible. Then each day the soldiers continue to make the position even more secure. Soldiers are trained to take the attackers' viewpoint, looking for vulnerabilities and guarding against them.

"Every day you're digging your foxhole and making it more secure," Bundt elaborated. "You're checking the perimeter of your defensible position. Then you send people out and they look from the enemy's point of view. They go through every position in your security area and try to detect if there's a vulnerability. Is there a spot where the enemy can approach unseen? We call that a dead zone. That's what makes things secure. We continue to improve our security posture. It comes through iteration."

That sort of intense focus on security has not been rewarded or encouraged in the private sector, where openness and ease of use are attributes that attract customers. As the attack plain begins to expand and digital attacks spread and become individual, physical, or even kinetic in nature, the calculus will change. When a digital hack or vulnerability can turn a trusted personal device—a laptop or automobile—into an improvised explosive device, the perception of vulnerability is radically altered.

How can designers strike the optimal balance between efficiency and security? As we know, complex systems are not just found in the world of technology, and it makes sense to look at older, more established complex systems to see how they have dealt with the issues facing today's designers.

What could we learn about efficiency from biology and life sciences?

"In biology every organism has evolved to a state that is efficient," said Kavita Berger, a molecular biologist at Gryphon Scientific, a small business that specializes in global health security, homeland security, preparedness, and science policy in Takoma Park, Md. "It is operating at efficiency in its environment, and when that environment changes, the organism changes. This is the driving force behind small and large genetic changes. Organisms adapt to

new environments. But they have developed redundancies for essential functions to make sure the organisms survive."

That's the paradox of efficiency in biological systems. Evolution forces organisms to be efficient, but to survive organisms also must have some level of redundancy. Those redundancies are essential because naturally occurring mutations may damage certain essential pathways, or a changing environment may make certain functions obsolete. Latent abilities and redundant systems enable organisms to survive and reproduce even in the face of those internal and external challenges.

However, that redundancy by definition makes the organism less efficient.

"In agriculture, farmers grow crops as monocultures, meaning a single variety of plant all of which have the same traits," Berger said. "If you had a field that had different varieties, with inherent diversity, then a pest might affect one group of crops but not the rest. You still have the ability to recover crops. This applies to almost any biological system."

What Are We Optimizing For?

Adapting that notion of redundancy as an essential part of a highly efficient system to engineered products is something engineers are beginning to grapple with.

"In engineering efficiency is a perfectly good concept, but it's a bounded concept that might not apply to the future," said Braden Allenby, president's professor of sustainable, civil, and environmental engineering at Arizona State University in Tempe. "The old way of looking at engineering might apply if I need to create a widget and make it as inexpensive as possible. But that concept might not be applicable if I'm working in an environment that is highly complex and cyberattacks are an issue."

Allenby argues that the shifting focus between efficiency and security is analogous to the one physicists make when they investigate matter at different scales. At the macro scale, Newtonian physics explains the world quite well. But as physicists investigate at smaller scales or try to understand the interaction between minuscule bits of energy and individual molecules or atoms, they need to turn to the tool kit of quantum physics.

"We need to figure out where our traditional idea about engineering and efficiency is appropriate and when it's not," Allenby said.

As we prepare for the future we must ask ourselves: What are we optimizing for?

Traditional engineering has long optimized for things like cost, efficiency, or simplicity. But going forward, engineers are going to have to value security just as much. Internet-connected machines and IoT-enabled devices will allow systems to do amazing things, but they also create opportunities for bad actors to turn these systems against us. If we are going to get the full use from these connected machines, engineers must take that threat into account and optimize for security. **ME**

"WE NEED TO FIGURE OUT WHERE OUR TRADITIONAL IDEA ABOUT ENGINEERING AND EFFICIENCY IS APPROPRIATE AND WHEN IT'S NOT."

— Braden Allenby
Arizona State University

BRIAN DAVID JOHNSON is futurist in residence at the Center for Science and the Imagination at Arizona State University in Tempe and a futurist and fellow at the consultancy Frost & Sullivan.