Cybersecurity Requires an Active Approach

SMT Prospects and Perspectives

by Dr. Jennie S. Hwang, CEO, H-TECHNOLOGIES GROUP

I last wrote about cybersecurity nearly 10 years ago in a column titled "Cybersecurity—from Boardroom to Factory Floor." So, where do we stand on cybersecurity? As the digital world continues pushing ahead, it comes with new challenges in the cyberspace. Individual systems and/or infrastructure systems are subject to attacks by increasingly savvy adversaries who can leverage new and emerging technologies.

A cyberattack can be surreptitiously detrimental, crippling business operations, the national economy and security, or just jeopardizing an individual laptop. This pervasive and persistent security threat is one of the most formidable challenges of our times.

In my 2013 column, I stated: "Cyberattacks will continue to be a huge concern to U.S. corporations in the foreseeable future. It's a matter of 'when' not 'if.' It is not industry-specific; every company will have to deal with this challenge. The earlier that preparation is made, the better a company is positioned to fend off the attack. The most insidious nature of a cyberattack is that it could happen anywhere at any time without physical boundaries across national borders." Indeed, potential hacking is timeless and borderless.

Under this backdrop, is it feasible to reach the level of being un-hackable? And what does it take to reach that level of security? Practically speaking, "un-hackability" is a relative term, which is a moving target as well. In other words, it relies on whether we can alleviate the weak and vulnerable link(s) in the system, set the strategy, and practice to outsmart and outpace the potential adversaries.

The foundational pillars behind an un-hackable system are hardware, software, data, computing, communication, human, and integration. Each of these pillars must surpass the anticipated capabilities of potential hackers. A holistic cybersecurity needs to embrace all types of security capabilities including:

- Critical infrastructure security
- Application security
- Network security
- Cloud security
- Edge (IoT) security

Also in my 2013 column, I mentioned, "Under a savvy and diligent governing board oversight, a cyber culture can be cultivated over time with persistent and pervasive effort by considering the following 20 actionable items." The 20th item called out in that article was to "Keep pace with emerging technologies."

The foundational pillars behind an un-hackable system are hardware, software, data, computing, communication, human, and integration.

Omnipotent Technologies

What are game-changing technologies behind the cybersecurity capabilities? Take artificial intelligence as an illustration. I'm reluctant to mention the phrase "artificial intelligence" as lately it has become household vernacular. However, AI brings "ammunition" against attacks. In practice, AI and computing power are intimately intertwined. With the recent acceleration of computing power, the advancement of AI is expected to gain momentum, although fundamental breakthroughs must still be made to reach the next level of performance.

This emerging technology also comes with risks as AI enables another level of attack abilities. The logical question is what the plausible strategies and methodologies are to integrate AI into the security infrastructure in a timely fashion that will fend off an AI-empowered attack. It is worth noting that defense is one thing and offense is another; one must be able to go on the offensive as well as defend.

Another illustration is quantum mechanics. While "quantum" has also been overused as well, it works here. A quantum computer's omnipotent computing power, in virtue of quantum's "quirky and spooky" nature of superposition and entanglement, can solve problems that are far too complex for classical computers and supercomputers to figure out in a finite timeframe. Even the processors with trillions of transistors are falling way behind.

The potential impact of quantum computing on cybersecurity is profound and is expected to transform cybersecurity and change the global landscape. Its anticipated capabilities pose a significant threat to cybersecurity infrastructure, as it can disrupt current encryption systems, requiring a change in how the data are encrypted. This includes solving the algorithms behind encryption keys that protect the data and the internet's infrastructure.

The public key cryptosystem, RSA, has been widely used for secure data transmission. As of now, not one individual, company, or country has reached or even is near to the level of the computing capability in qubits required to totally disrupt the current encryption system. Reportedly, a quantum computer would need to be as large as 70 million qubits to break that encryption. IBM[1] and Google[2], among others, have roadmaps to achieve 1 million qubits by 2030. Nonetheless, indisputably, a leader in quantum computing holds the omnipotent key. The competitive race is fiercely marching on.

Global Race

Speaking of the race, in 2016 China blasted the world's first quantum communication satellite into orbit from the Gobi Desert. "The newly-launched satellite marked a transition in China's role—from a follower in classic information technology (IT) development to one of the leaders guiding future IT achievements," said Pan Jianwei, chief scientist of Quantum Experiments at Space Scale (QUESS) project with the Chinese Academy of Sciences (CAS)[3]. With the help of the new satellite, scientists are testing quantum key distribution between the satellite and ground stations and conducting secure quantum communications. QUESS is designed to establish "hack-proof" quantum communications by transmitting uncrackable keys from space to the ground and provide insights into the strangest phenomenon in quantum physics—quantum entanglement.

Quantum communication boasts ultra-high security by exploiting the quirky properties of subatomic particles, as a quantum photon can neither be separated nor duplicated. Thus, it is impossible to wiretap, intercept, or crack the information transmitted through it.

In upcoming decades, it remains to be seen who will win the quantum computing or quantum communication. All embracingly, it appears to indicate that the disruptive quantum computing abilities are still many years away. One thing for sure is that we must address security in the quantum world. This is valid and critical.

The Role of Hardware

For our industry, it would be remiss not to call out hardware. Hardware technologies to increase the bandwidth and capacity within the desired power and thermal envelope, including processor, memory, GPU, interconnect, among others, make the applications of AI feasible. In hardware chips, the system design, development, manufacturing, and the supply chain that enable the functions and performance of the omnipotent technologies are the critical part of the equation. On top of hardware for machine learning, the hardware for "deeper" learning abilities requires integrating the natural language processing and neural network that mimic the functionality and connectivity of neurons in the human brain in the hardware system, which is yet to evolve.

> In hardware chips, the system design, development, manufacturing, and the supply chain that enable the functions and performance of the omnipotent technologies are the critical part of the equation.

Other Than Technologies

To defend against hackers (human, machine, human-machine teaming), in addition to technologies, other key elements of establishing a resilient cybersecurity system include people talents, sound policies, and effective processes to tackle the challenges of the complex and ever-changing cyber-physical-human infrastructure.

In a nutshell, to be un-hackable, always be on the lookout for new and innovative ways to stay one step ahead of hackers—not only to react, but to anticipate and to envisage. **SMT007**

Reference

1. "IBM plans a huge leap in superfast quantum computing by 2023," by Robert Hackett, *Fortune Magazine*, Sept. 15, 2020.

2. "Quantum computing is entering a new dimension," by Robert Hackett, *Fortune Magazine*, Dec. 3, 2020.

3. "What the World's First Quantum Satellite Launch Means," by Robert Hackett, *Fortune Magazine,* Aug. 16, 2016.

Appearances

Dr. Hwang will deliver two professional development courses: "Solder Joint Reliability—Principle and Practice," from noon to 3 p.m. Jan. 22, and "Preventing Product Failure and Manufacturing Defects," from 1:30 to 4:30 p.m. Jan. 23, at IPC APEX EXPO 2023 in San Diego, California.

Dr. Jennie S. Hwang—an international businesswoman and speaker and a business and technology advisor—is a pioneer and long-standing leader to SMT manufacturing since its inception as well as to the development and implementation of lead-free electronics technology. Among her many awards and honors, she was inducted to the International Hall of Fame–Women in Technology, elected to the National Academy of Engineering, named an R&D Star to Watch, and received a YWCA Achievement Award. Having held senior executive positions with Lockheed Martin Corp., Sherwin Williams Co., and SCM Corp., she was the CEO of International Electronic Materials Corp. and is currently CEO of H-Technologies Group, providing business, technology, and manufacturing solutions. She has served on the board of Fortune-500 NYSE companies and civic and university boards; the Commerce Department's Export Council; the National Materials and Manufacturing Board; the NIST Assessment Board; as the chairman of the Assessment Board of DoD Army Research Laboratory and the chairman of the Assessment Board of Army Engineering Centers; and various national panels/committees and international leadership positions. She is the author of 600+ publications and several books and is a speaker and author on trade, business, education, and social issues. Her formal education includes four academic degrees, as well as the Harvard Business School Executive Program and Columbia University Corporate Governance Program. For more information, visit JennieHwang.com. To read past columns, click here.

U.S. Departments of Labor, Commerce Announce 120-Day Cybersecurity Apprentice Sprint to Promote Registered Apprenticeships

At a National Cyber Workforce and Education Summit at the White House, Secretary of Labor Marty Walsh and Secretary of Commerce Gina Raimondo announced the 120-Day Cybersecurity Apprenticeship Sprint, an effort to support numerous industries' use of Registered Apprenticeships to develop and train a skilled and diverse cybersecurity workforce.

The 120-Day Cybersecurity Apprenticeship Sprint supports a commitment to expand Registered Apprenticeships to meet industry's need for talent and to connect underserved communities to good jobs. Improving the nation's cybersecurity apparatus is critical to the nation's economic and national security.

The partnership between the departments of Labor, Commerce, other federal agencies and the White House Office of the National Cyber Director seeks to recruit employers, industry associations, labor unions, educational providers, community-based organizations and others to establish Registered Apprenticeship programs or to join existing programs to ensure the nation's economic sectors have greater numbers of qualified cybersecurity workers. The sprint will continue until National Apprenticeship Week, Nov. 14-20, 2022.

There are currently 714 registered apprenticeship programs and 42,260 apprentices in cybersecurity-related occupations. Since Jan. 20, 2021, 199 new programs have been created – a 28 percent increase during the Biden-Harris administration. The 120-Day Cybersecurity Apprenticeship Sprint will build upon this progress and focus on creating new pathways for workers in cybersecurity or a related field through partnerships with K-12, higher education, workforce partners and training programs. Introducing more employers to the potential of cybersecurity Registered Apprenticeships is essential to fill the nearly 700,000 open cybersecurity jobs, which span all industries.

(Source: U.S. Department of Commerce)