The 348th Engineer Battalion prepares for mobilization at the Total Force Training Center, Fort McCoy, Wisconsin, in late May. Experts share that sensors and other Internet of Things devices will be able to be placed everywhere—in concrete, glass or fabrics, for example.

Internet of Things Invasion

Acknowledging the inevitable IoT deluge may be only a starting strategy for the military.

BY KIMBERLY UNDERWOOD

As the number of electronic devices connected to the Internet grows, so does the security risk and the chance of data exfiltration by adversaries. Warfighters' use of Internet of Things devices makes the military increasingly vulnerable, experts say. In addition, as the concentration of smart sensors and connected tools widens, the military may not be able to conduct unexpected operations. And the strategy of how to harness so-called IoT devices by the military becomes a more complex decision-making process, explains Don Codling, USMC (Ret.), an international cybersecurity advisor and former FBI unit chief in the cyber division, and David Bray, cybersecurity, Internet leader and advisor to the Defense Department, as well as executive director, People-Centered Internet.

"The consumer IoT market is just going a million miles an hour," notes Codling, who spent 23 years working international cyber crime at the FBI. "But in my opinion, a lot of the consumer-grade IoT devices are going to be absolutely, I hate to say, useless. If you can't change the password, if you don't have any encrypted channels, if they are promiscuous in how they try to connect with other devices, I would think that the most anybody who's in information security would say is, 'Keep that away from me.'"

"Essentially, what is happening is that we are instrumenting the planet in ways that have never happened before," Bray adds. "It's completely unprecedented. And from the military's perspective, I think the first thing is to recognize that it is going to happen. It is something you need to take into account in your military planning. Whether you want it to happen or not, it is going to happen."

Bray, who began working for the U.S. government at age 15 creating computer simulations at a high-energy physics facility and has multiple degrees from Emory University including a doctorate from the Goizueta Business School, warns that smart sensors will be everywhere.

"When you look at the future of the Internet of Everything, it's going to be baked into concrete; it's going to be put into glass; it's going to be put into

Russell Gamache

textiles and fabrics," he says. "Smart infrastructure could be in factory floors or in the ground below, sensing vibrations, or sensing electromagnetic activity, or a whole range of signatures." In addition, subcutaneous sensing tools could be placed in people.

The number of devices is staggering, he emphasizes. "We hit the tipping point back in 2013 when nobody realized that there were 7 billion people on the planet and 7 billion networked devices, and it doubled two years later to 14 billion," Bray suggests. "Now we are at 25 to 35 billion devices. If we assume that will double in six years, which is probably more than conservative, at a minimum there's 10 times as many networked devices than there are people, which raises huge questions from a cybersecurity perspective or an information and influence operations perspective."

Don Codling, former FBI unit chief, Cyber Division, warns that it is going to become increasingly difficult to lock down the security of Internet of Things devices.

The inundation of Internet-connected sensors presents both an opportunity and potential calamity to the military, the experts say. IoT tools will make it harder for adversaries to mask their presence. Devices will help provide an early warning of activities of importance for the military to address. IoT instruments can perform monitoring tasks usually completed by warfighters or expensive space-based assets, Bray explains.

The inherent insecurity of consumer-grade IoT equipment does offer an advantage to the U.S. military. "You can exploit that if your adversary or your target is not using good cyber hygiene," Codling says. "You can exploit their devices to have a sensing capability."

However, as a double-edged sword, the risks of IoT devices are great. "The vulnerability is what is going to keep people awake, because you'll have certain IoT devices that you are going to have absolutely no idea that they're even there," the former FBI unit chief warns. "A lot of the devices that [warfighters] use were never designed to be a secure communications link. It doesn't have encryption. It doesn't have audit capability. It doesn't have system logs. It doesn't have all these kinds of things. So if you're a young Marine lieutenant, let's say, or an officer, you're carrying around your private cellphone and you are texting back and forth and you've got your Fitbit. And then you have your iPad that you're going to bring with you on deployment to FaceTime [family members]. The list of devices just goes on and on. And the number of things now that an adversary can use to data mine on you to figure out what you're doing is [only growing]."

Because of the prevalence of IoT equipment, the U.S. military may not be able to perform operations in the future without being detected. "It's just going to get harder," Bray warns. "If I were the military, I would be planning for it to be very difficult to do actions without detection five years, 10 years from now. And that includes subsurface activities in the ocean and special operations on land."

Moreover, the military must be aware of the unintended consequences of any of its commercial off-the-shelf (COTS) equipment, as the devices can be put to use in other, unexpected and detrimental ways. "Most of these things are designed with zero thought for security," Codling continues.

"You could have a general officer or soldier in a conference room and you put up two smart TVs, you'd better make darn sure that those TVs are not calling out to Samsung or Huawei or anyone else. You have to now consider, 'Is that really a secure conference room?' If you start bringing in other devices, then the answer is usually no. And that's why you have to be very, very conscious of what sorts of material, what sorts of equipment you put into place."

Bray adds that the influx of IoT makes it easier for adversaries to create deception. "What happens if somebody tricked some of these devices to claim you did something that you actually didn't do, for military purposes?" he asks. "If someone wants to make it look like you did some incident that you actually didn't do, you'll be caught in the loop saying, 'I didn't do it.'"

When combined with information from the numerous data breeches over the last several years, IoT devices give adversaries a key surveillance tool for information warfare. "The OPM [Office of Personnel Management] breach of 2015, which impacted an estimated 23 million people, was certainly ripped off by China," Codling says. "And a lot of that was so they could build a very rich profile of us."

"We are instrumenting the planet in ways never seen before," says David Bray, Defense Department consultant, as well as executive director, People-Centered Internet.

With those profiles, adversaries can then use IoT equipment to hone in on activities. "If an adversary is super focused on you and all of a sudden you're not using that phone anymore, all of a sudden you're not doing the same kinds of thing. That indicates to them that either you've gone dark or you've switched devices," Codling notes. "So now I need to go and wiretap your girlfriend's stuff or start monitoring your parents. That's the next logical thing to do. I start to figure out when you're going to come back up for air. You almost have to make it a sterile [communications] environment, like in a scif. I think that's the world we're heading into. And it's going to become increasingly difficult to lock that down."

Another key consideration for the military is that most IoT devices will not come from U.S. companies—including traditional defense partners—so Bray recommends that the United States find allied partners that can build IoT devices, as products from China are not an option. "Probably a lot of these IoT devices ultimately will not be manufactured in

the United States, which raises questions about if can you trust a device," he states.

The prevalence of COTS devices may force the military's hand towards the use of IoT devices. "The military is increasingly going to have to rely on taking what might be IoT devices that are built for consumer purposes and think about how they can either incorporate them in ways that are useful towards its assets, or disassemble them and add in special components to help it augment what it needs to do for military purposes," Bray suggests.

Here, one potential solution is to rely on zero trust networks, he advises. In this case, users assume that there are nodes on their networks from devices that cannot be trusted. "If you assume a stance of 'there is no trusted layer, there is no trusted enclave,' then you identify the patterns of behavior. Is this device doing something that is odd? Is it trying to gain access to things that normally it should not? It really is about shifting from assuming there are things that are trusted enclaves and signature detection of malware to go into patterns of life and behavior and having ways in which the different nodes in your network can help identify who and what they can trust."

As a tool, splicing, where users have a virtual cloud of nodes on a network that only they can see, offers potential, Bray says. "Splicing may or may not become a reality, but what is really behind it is this idea of specifying nodes of trust, versus nodes that you don't want to trust. Software-defined networks are obviously going to play into this too," he adds.

Once the devices are fortified, the art of selecting what kind of IoT tool to use will become part of the military's strategy. "There is going to be this convergence of being able to rapidly perceive information at a distance and being able to remotely produce effects," Bray offers. "It really is about having smarter access to things that are happening with your assets, with your bases, with your people, your facilities, and being able to have what some would call the equivalent of digital twins, that are able to inform and give you an informational advantage as to what is occurring, and at the same time being able to send effects back. That is why the military should care about what is happening [with IoT devices]."

• • • — • —

To share or comment on this article go to ***http://url.afcea.org/November19***

contact: Kimberly Underwood, kunderwood@afcea.org