Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

4 Reasons Why the Internet of Everything Will Require a New Breed of IT Pros

SUDARSHAN KRISHNAMURTHI

Learning Outcomes

After reading this article, you will be able to:

- Give a fundamental description of the Internet of Everything (IoE).
- Appreciate the crucially heightened role of data analysis as the IoE grows.
- Identify the many emerging roles in the future for the IoE.

Like many products and services we enjoy today, the Internet's origins rest within the halls of government.

The Advanced Research Projects Agency Network, which laid the technology foundation for how the Internet works, was originally funded by the Defense Department. Just a few decades later, that foundation has been built upon to create an entity only the most visionary thinkers could have imagined: the Internet of Everything.

IoE is an interconnected web of systems that brings together people, processes, data and things. There are currently over 20 billion connected devices, representing less than 1 percent of physical objects. Cisco predicts that by 2020, 50 billion devices will be connected.

IoE's ubiquity and scale are even now producing data-derived insights that promise gains in productivity, new revenue streams and cost savings.

However, these changes cannot occur without a new breed of trained IT professionals.

1. Analysis is Key

With IoE, the network will play a more crucial role than ever. It will need to be more secure, agile, context-aware, automated, dynamic, and programmable. The realms of mobile, cloud, apps, and big data and analytics will all be interconnected in IoE. Security will be of particular concern; with so many devices all connected, the attack surface will increase exponentially, and security breaches could become even costlier.

The amount of data generated by and exchanged among this ever-growing number of devices will require analysis. The role of the data scientist will therefore be crucial in terms of converting this data into usable information.

Government agencies stand to gain dramatically from the improvements in data gathering and streamlined workflows. In short, IoE is about connecting people, process, data, and things; ensuring the connections are secure; and making the network programmable so information gathered from data can be more intelligently applied to devices rather than having to configure and manage them manually.

2. The Network is Expanding

IoE makes important connections that reveal actionable insights, but it also will create significant challenges for the workforce—in terms of both security and data handling issues and adequate training. Getting prepared for IoE will require the existing workforce—especially in areas such as manufacturing, safety and security, utilities and transportation—to understand IT networking to a greater degree.

At the same time, IT networking professionals need to better understand manufacturing-control systems and industrial networks as IoE will cause these operational technologies to converge with IT. And lastly, it will be vital for the current generation of students coming out of college to have the networking skills that will enable them to address this convergence.

The traditional networker's view is expanding to include many new technologies, and the networker's responsibilities are expanding to include many new duties. For example, the increase n connected things requires network professionals to maintain a strong security posture across the expanded attack surface.

Also, the ability to analyze big data and turn it into actionable information is needed to drive business outcomes. There re many emerging roles in the future for IoE: businessransformation specialists, cloud brokers, network programners, and data scientists. Cybersecurity becomes more pervasive nd the networking career becomes much more specialized.

3. Training Is Only Half the Battle

he transition to IoE is not only desirable but inevitable, and e people best suited to lead that transition are those with undamental networking experience. That is because they are quipped with the knowledge to build the bridge from network frastructure to the application environment. Agencies will eed to work with industries throughout the world to create the athway for IT networking skills and talent development. Con- ued efficiency and productivity gains will depend upon it.

Training current IT employees is half of the battle. The other lf of the educational battle is to prepare youth from the beginng to understand the network and its underlying connection everything. It is incumbent on IT companies to work with iversities, secondary schools, networking academies, and arning partners to develop curricula to ensure rising talent is ell prepared to understand the functioning of the network and w it makes IoE work.

Because IoE will eventually affect all government entities, ployees of those entities must be properly trained in manng the network as IoE's basic platform. The evolution is eady well under way, and the demand for networking talent already being felt. Beyond understanding network deploynt and operation, those at the forefront of the change will be ng the network in new directions, using 21st-century skills he process: critical thinking, complex problem solving, data lysis, and communication and collaboration.

New Workers Ditch the aditional

dents' needs and preferences regarding where and when will get training are changing, along with what they are learning, because of new bring your own device policies, and ubiquitous access models of education. Students no longer prefer traditional delivery modalities. Instead, they want mobile, video-based, game-based learning that not only is an evolution of traditional delivery but also helps remove barriers to education by making it easy, fun, accessible, and effective. A 2013 survey of Cisco-certified professionals revealed a strong preference for hands-on practice labs, simulations, and video-based training. Rather than attending a class on each of these subjects, this core knowledge set will be available in real time on an as-needed basis to aid in decision-making.

It is incumbent upon government agencies to strategically forecast the needs of their constituents and develop plans to best meet those needs. The network demands of IoE require a shift in how the current and future workforces are educated to fill critical gaps. With a properly equipped staff of network professionals, agencies will be able to fully realize the benefits of IoE: faster and more efficient services, greater productivity and cost savings.

Critical Thinking

1. Why does the IoE's expanded attack surface present a particularly serious concern?
2. In what ways will government agencies gain dramatically from the improvements in data gathering and streamlined workflows?
3. For the upcoming generation, how early in their education should IT instruction begin? Explain.

Create Central

www.mhhe.com/createcentral

Internet References

Goldman Sachs: "The Internet of Things: The Next Mega-Trend"
http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/index.html

InformationWeek: "Cisco Futurists Plan For Internet Of Everything"
http://www.informationweek.com/big-data/big-data-analytics/cisco-futurists-plan-for-internet-of-everything/d/d-id/1108286

Yahoo! Finance: "What the 'Internet of Things' Means for Enterprising Entrepreneurs"
http://finance.yahoo.com/news/internet-things-means-enterprising-entrepreneurs-234500396.html

han Krishnamurthi, "4 Reasons Why the Internet of Everything Will Require a New Breed of IT Pros," *nextgov.com*, July 25, 2014. Copyright © 2014 by National Journal Group.
hts reserved. Used with permission from Wright's Media.

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

Next Generation of Cyber Defenders Prepare for Expanding Battlefield

While private-sector cybersecurity flaws, such as the recent Microsoft Internet Explorer hack, dominate headlines, college-level cybersecurity competitions have become a major training and recruiting ground to supply the growing cybersecurity need.

KARIS HUSTAD

Learning Outcomes

After reading this article, you will be able to:

- Describe the annual Raytheon National Collegiate Cyber Defense Competition (NCCDC).
- Acknowledge the current (and rapidly growing) "human capital crisis" in cyber security.
- Recognize the challenges of creating a cyber-talent pipeline.

When reigning champion of the Raytheon National Collegiate Cyber Defense Competition (NCCDC) and current Rochester Institute of Technology (RIT) senior Lucas Duffey heard about the Target hacks, he could only pity the multibillion dollar company.

"It was kind of sad," says the computing-security major. "A lot of us look at these things and say 'Why did that have to happen in the first place?' "

Listen up, Target. Mr. Duffey is soon to be the first line of defense against the growing threat of cyber attacks.

The need for an increase in the cybersecurity workforce has been apparent for some time—a 2010 Center for Strategic and International Studies (CSIS) study announced there was a "human capital crisis" in cyber security, with an outstanding need for 10,000 to 30,000 trained workers. While this study and others called for a more robust military cyber defense, this year has caught the private sector on its heels. High profile attacks such as the Target credit card breach, which left more than 70 million cards compromised, and numerous other vulnerabilities have ramped up the demand for high quality cyber defenders. This, in turn, has created a surge of interest in competitions that are recruiting and training the next generation of cyber defenders, one simulated hack at a time.

"[NCCDC] is definitely very stressful," Duffey says. "Your systems are going down all the time."

The competition, which has taken place in San Antonio, Texas, every year since 2004, brings 10 universities from regions across the country together for a three-day competition. Each team is put in charge of a fictional small tech company with 50 or more users, 7 to 10 servers, and common Internet services, such as mail servers and e-commerce. Over 17 hours, teams are scored on their ability to keep servers running, respond to customer inquiries (such as "Can you reset my password?"), and balance security with business.

Then there is the Red Team. This is a group of hackers whose sole purpose is to dismantle the other teams' security by running denial of service attacks and hacking customer passwords.

Duffey says his team practiced for hours every day in the months leading up to the competition, even skipping spring break vacations to learn operating system configurations and researching likely hacker targets. But he says the competitions provide incentive for that sacrifice.

"A lot of material you learn in school is very watered down," Duffey says. "The great thing about security competitions is that they give you pretty much every challenge you could see in a very short amount of time. . . . It pushes you to research on your own time."

Despite its grueling nature, the competition has only ecome more popular among students and schools. In 2006, 4 universities participated. During the 2014 regional and ational competitions, more than 180 universities were represented and more than 2,000 students participated. Sponsors, ho range from Goldman Sachs and the US Army to Microsoft which recently has dealt with a high-level vulnerability with its ternet Explorer browser), heavily recruit student competitors.

That's because need for trained cyber defenders has skyrocked since the first NCCDC competition and 2010 CSIS report. urning Glass Technologies monitors the supply and demand r cybersecurity jobs and found that between 2007 and 2013, bersecurity job postings grew 74 percent, but postings took percent longer to fill than normal information-technology bs and 36 percent longer than postings in general.

The private sector discovered its need the hard way. PricewaterhouseCoopers's 2014 Global Economic Crime Survey found at over the last three years, 7 percent of US organizations lost re than $1 million each to cybercrimes, and 19 percent lost tween $50,000 and $1 million.

"This is no longer a back-room discussion, this is a boardom discussion," says former Air Force Gen. Harry Raduege, irman of the center for cyber innovation at Deloitte, a preus top-level sponsor of NCCDC, and co-chair of the CSIS mmission. "Frankly, some progress had been made, but there an obvious need for much much more."

General Raduege says there aren't enough workers that have combined science, technology, engineering, and math trainneeded to effectively build cybersecurity-specific skills, ecially when technology is refreshing every year. He adds the need is also diversifying. From cyber attack insurance nts to cyber fluent communications officers, Raduege says the need to get the next generation of workers cyber-ready nds even beyond information technology.

"We need attorneys who know the difference between a botnd a spearfish . . . but can also explain that to a judge and y," he says.

owever, creating a cyber-talent pipeline isn't without its enges. Raytheon, a defense company and top sponsor of year's NCCDC, and Zogby Analytics conducted a survey illennials on cybersecurity, and found 82 percent of young s ages 18 to 26 had never had a high school teacher or nce counselor suggest a cybersecurity career. Less than ercent are even interested in a cybersecurity job. That er drops to 14 percent for young women.

e teach our young children right from wrong, and I think ed to do this specifically in their [digital] connectedness," eff Jacoby, a director for Raytheon intelligence, informand services. "The term 'cyber' has not made it into the ream [careers]."

Mr. Jacoby's solution? Advance education and awareness as early as possible.

For example, Raytheon sponsors a scholarship for elementary school teachers who innovate ways to teach STEM concepts, in addition to sponsoring numerous competitions.

"[Competitions are] really a way for colleges and universities to assess their own cyber security programs to make improvements," he says.

These early initiatives could be paying off. For Duffey, his interest in cybersecurity started with competitions in high school and continued when he joined RIT's Security Practices and Research Association (SPARSA), which runs its own national cybersecurity competition. The competition, he says, is key.

"When you look at other fields, like sports, [there's a football] quarterback—it is kind of sensationalized. People look up to these people," Duffey says. "I think something really important is having some milestones people can shoot for to get recognition."

The 2014 competition, which took place this weekend, at least had one storybook championship moment: The underdog won. University of Central Florida, who participated in the competition for the first time last year, beat RIT for the top prize.

Critical Thinking

1. Why has the competition become increasingly popular despite its grueling nature?
2. Do schools need to be held accountable for the findings that 82 percent of young adults (ages 18–26) never heard about a cybersecurity career from a teacher or guidance counselor? Explain.
3. Should an NCCDC champion be "sensationalized" the way a school's star quarterback is? Why or why not?

Create Central

www.mhhe.com/createcentral

Internet References

Business Journals: "2014 CyberPatriot National Youth Cyber Defense Competition Draws More Than 2,100 Teams, Breaks All Time Registration Record"

http://www.bizjournals.com/prnewswire/press_releases/2014/10/20/DC40841

ClearanceJobs: "How to Prepare for a Career in Cyber Security"

http://news.clearancejobs.com/2013/12/10/prepare-career-cyber-security/

Technical Education Magazine: "National High School Cyber Defense Competition"

http://techedmagazine.com/node/2529

WHNT: "Grissom High Team Takes Top Spot in National Cyber Defense Competition"

http://whnt.com/2014/04/06/grissom-high-team-takes-top-spot-in-national-cyber-defense-competition/

Hustad, Reprinted with permission from the April 29, 2014 issue of *The Christian*

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

Why Computers Won't Be Replacing You Just Yet

A 25-Question Twitter Quiz to Predict Retweets

SENDHIL MULLAINATHAN

Learning Outcomes

After reading this article, you will be able to:

- Understand how algorithms find information in unexpected places, uncovering "signal" in places we thought contained only "noise."
- Recognize big-data tools as having boundaries in which they excel and beyond which they can do little.
- Discuss the principle of "correlation is not causation" as one of the oldest of statistical problems.

Three computer scientists, Chenhao Tan, Lillian Lee, and Bo Pang, have built an algorithm that also makes these guesses, as described in a recent paper, and the results are impressive. You can think of the pair of Gore tweets as a practice round for a 25-question quiz that The Upshot has created based on their algorithm. (The answer: Gore's first tweet got more retweets).

That an algorithm can make these kinds of predictions shows the power of "big data." It also illustrates a fundamental limitation of big data: Specifically, guessing which tweet gets retweeted is significantly easier than creating one that gets retweeted.

To see why, it is useful to see how the algorithm was built. It used a data set of around 11,000 paired tweets—two tweets about the same link sent by the same person—to learn which word patterns looked predictive and then tested whether these patterns hold in new data. This is usually how "smart" algorithms are created from big data: Large data sets with known correct answers serve as a training bed and then new data serves as a test bed—not too differently from how we might learn what our co-workers find funny.

The end result is an algorithm that guesses well. It can guess which tweet gets retweeted about 67 percent of the time, beating humans, who on average get it right only 61 percent of the time.

This is striking when you think of the enormous handicap the algorithm has. Yes, it could learn from 11,000 pairs of tweets. But it has no other knowledge. It has none of the wealth of contextual information you have accumulated over the years. It has never heard friends' complaints about spouses checking their phone the first thing in the morning. It does not have a sense of humor or know what a pun is. It does not know what makes a turn of phrase elegant or awkward.

It must rely on a few crude features, such as length of the tweet, the presence of certain words ("retweet" or "please") or the use of indefinite articles. Yet with so little, it does so much. This is one of the miracles of big data: Algorithms find information in unexpected places, uncovering "signal" in places we thought contained only "noise."

But we do not need to roll out the welcome mat for our machine overlords just yet. While the retweet algorithm is impressive, it has an Achilles' heel, one shared by all prediction algorithms.

We care about predicting retweets mainly because we want to write better tweets. And we assume these two tasks are related. If Netflix can predict which movies I like, surely they can use the same analytics to create better TV shows. But it doesn't work that way. Being good at prediction often does not mean being better at creation.

One barrier is the oldest of statistical problems: Correlation ot causation. Changing a variable that is highly predictive have no effect. For example, we may find the number mployees formatting their résumés is a good predictor of ompany's bankruptcy. But stopping this behavior hardly ns like a fruitful strategy for fending off creditors.

he causality problem can show up in very subtle ways. For mple, the tweet predictor finds that longer tweets are more y to be retweeted. It seems unlikely that you should there- write longer tweets. The old adage that "less is more" is, ything, truer in this medium. Instead, length is probably a d predictor because longer tweets have more content. So lesson is not "make your tweets longer" but "have more ent," which is far harder to do.

nother problem comes from an inherent paradox in pre- ng what is interesting. Rarity and novelty often contribute nterestingness—or at the least to drawing attention. But an algorithm finds those things that draw attention and s exploiting them, their value erodes. When few people omething, it catches the eye; when everyone does it, it is um. Calling a food "artisanal" was eye-catching, until it me so common that we're not far away from an artisanal ger.

the Twitter example, the use of the words "retweet" or se" were predictive. But if everyone starts asking you to re this article. Please," will it continue to work?

nally, and perhaps most perversely, some of the most pre- ve variables are circular.

r example, in another paper, the computer scientists Lars strom, Jon Kleinberg, Lillian Lee and Cristian Danescu- lescu-Mizil predict which posts on Facebook generate comments. One of the most predictive variables is the it takes for the first comment to arrive: If the first comment es quickly, then the post is likely to generate many more ments in the future. This helps Facebook decide which to show you. But it does not help anyone to write a highly ented post. It says: "Want to write a post people like? write one that people like!"

ese limitations are not meant to take away from the of predictive algorithms. It is truly amazing, for exam- ow well an algorithm can predict which tweets will get eted.

It does remind us to moderate expectations. Arthur C. Clarke once posited three laws of prediction. The third is apropos here: "Any sufficiently advanced technology is indistinguishable from magic." Because algorithms armed with big data can do some impressive things—self-driving cars!—we can too easily treat them like magic and overstate what they do. This can lead to extrapolations that are simply not realistic. (Soon computers will be doing my job!) It can create fears that are ill-founded. (Soon companies will know enough about me to get me to buy anything!) It can create expectations that we are very far from meeting. (Soon computers will write movies!)

The new big-data tools, amazing as they are, are not magic. Like every great invention before them—whether antibiotics, electricity, or even the computer itself—they have boundaries in which they excel and beyond which they can do little.

Critical Thinking

1. With relevance to this article, expound on the statement, "Being good at prediction often does not mean being better at creation."
2. Explain the purposeful difference between "make your tweets longer" and "have more content."
3. What does it mean that "some of the most predictive variables are circular"?

Create Central

www.mhhe.com/createcentral

Internet References

Atlantic: "Why Computers Will Never Replace Us"
http://www.theatlantic.com/technology/archive/2011/08/why-computers-will-never-replace-us/243818/

LA Daily News: "Ted Lieu and Paul Weber: Computers can't replace human judgments here"
http://www.dailynews.com/opinion/20100819/ted-lieu-and-paul-weber-computers-cant-replace-human-judgments-here

Value Line: "Computer Can't Replace Human Insight"
http://www.valueline.com/Stocks/Computer_Can%E2%80%99t_Replace_Human_Insight.aspx#.VGeedGfp9X0

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

From Smart House to Networked Home

Two foresight specialists describe how tomorrow's integrated, networked, and aware home systems may change your family life.

Chris Carbone and Kristin Nauth

Learning Outcomes

After reading this article, you will be able to:

- Recognize that new technologies follow an adoption curve from niche to mainstream.
- Recognize that it is the interaction of technological advances and societal drivers that determine which technologies go mainstream.
- Recognize that advances being made across several broad technical areas are what eventually lead to new commercial products.

In the last decade, a range of digital technologies and services have hit the market and moved quickly from niche use to the mainstream. Consider that just seven years after being founded, Facebook is used by more than 50% of the online population in the United States and India, and much higher percentages in global markets from Chile to South Africa to Indonesia. And flat-panel TVs, e-readers, smartphones, and even augmented-reality apps—all largely missing from the consumer landscape just a few years ago—continue to be eagerly adopted even in the face of economic uncertainty.

As we look toward the next decade, it's clear that we are in for even more dramatic changes in the roles that technology will play in daily life. But what technologies are poised to move from niche toward the mainstream in the next 10 years? And how will these technologies change everyday activities?

To bring this into sharper focus, Innovaro Inc.'s futures consulting group identified 10 key themes that it feels will help define the tech experience in the coming decade. These 10 "technology trajectories" will give people a powerful new "toolkit"—new devices, services, and capabilities—that will forever alter the way that we go about everyday activities, from dating and shopping to learning and working.

This glimpse of Innovaro's 10 Technology Trajectories presents several forecasts for how these new capabilities could reshape family and home life in the next decade. And although these themes were identified with the United States and other advanced economies in mind, the Technology Trajectories have global potential to reshape life in emerging economies as they're adopted and explored there as well.

10 Technology Trajectories

1. **Adaptive Environments.** Advances in materials will make the home and work environment "smart." Everyday objects, surfaces, and coatings will gain the ability to adapt to changing conditions or people's needs (e.g., becoming self-cleaning, self-insulating, or protective). The built environment will no longer be simply structural and passive; it will become adaptive, functional, and smart.
2. **Cloud Intelligence.** The cloud will evolve from being a static repository of data into an active resource that people rely on throughout their daily lives. With new capabilities for accessing online expert systems and applications, we'll tap into information, analysis, and contextual advice in more integrated ways. Virtual agents will migrate from being an automated form of phone-based customer service to a personalized form of support and assistance that provides information and—more importantly—performs useful tasks. For example, such agents might design a weekly menu based on a family's health profile, fitness goals, and eating preferences, and automatically order ingredients.

3. **Collaboration Economy.** The power of collective intelligence will enable us to accomplish cognitive tasks not easily handled by virtual agents and machines in the cloud. We'll get advice and recommendations and solve problems by tapping into the social graph, and this cognitive outsourcing will be applied to both business issues and personal and lifestyle questions (e.g., "Which diet will work best for me?").
4. **Contextual Reality.** People will navigate through their daily activities thanks to multiple layers of real-time and location-specific information. This contextual overlay for everyday life will give us a new way to see our surroundings and provide new forms of decision support. We will move from a world where information and connections are hidden to one where real-time, contextual information generates ambient awareness.
5. **Cutting the Cable.** Personal devices will be largely untethered from wired power and data connections. Access to the Internet will be ubiquitous, and the tech infrastructure—from electronics to sensors to cars—will be powered by a more diverse set of technologies, including micro-generation, wireless power transmission, and advanced power storage. We will move beyond plugging in, and even beyond the "plug and play" model, to a world where data, power, and inter-networking are ubiquitous.
6. **Information Fusion.** It will become possible for people to generate useful insights about their own habits and behaviors by fusing personal data (e.g., social media profiles, tweets, location data, purchasing histories, health sensor data). But these insights will only be as good as a user's ability to understand and act on them. Personal data will become comprehensible through visualization and other services.
7. **Interface Anywhere, Any Way.** Intuitive interfaces will become the dominant form of interaction with personal electronics and computing devices. We'll be freed from the rigidity of conventional input devices (e.g., keyboard, mouse, screen, remotes) and able to interact with the digital world anywhere—and any way—using a combination of gesture, touch, verbal commands, and targeted use of traditional interfaces.
8. **Manufacturing 3.0.** Manufacturing will be reconceived—from a far-flung, global activity to more of a human-scale and re-localized endeavor. As consumers continue to call for both personalization and attention to environmental pressures, demand will grow for a more local manufacturing infrastructure where product schematics in certain categories are digitized and distributed to commercial tabbing services (or in-home 3-D printers) for final fabrication.
9. **Personal Analytics.** Data analytics will increasingly become a consumer tool as much as a business tool. This will open up analytics to a wide variety of personal and lifestyle applications. We'll collect, store, interpret, and apply the vast amounts of data being created by and about ourselves during our everyday activities.
10. **Socially Networked Stuff.** Many of our possessions will interact with each other and with the broader digital infrastructure. This will create a world of socially networked stuff, where things can actively sense, communicate, and share data. Rather than owning a fragmented set of possessions and devices, passively sitting next to each other, we'll manage a dynamic ecosystem of belongings that interact and work in concert for our benefit.

Societal Drivers Influence Technological Advancements

So, how will the new capabilities described in the 10 Technology Trajectories change home and family life? What will our homes look and feel like? How will they support our activities and lifestyles?

Technology is not the only driver at play here, and the Technology Trajectories are not emerging in a vacuum. There are numerous social, generational, and values drivers at play as well. Of the many drivers that our team at Innovaro considered while generating these forecasts, we especially noted the impact of digital natives on adoption of technology in the home, shifting demographics, and economic considerations.

- **The maturing of the digital natives.** Digital natives—people who have grown up never knowing a world without the Internet, smartphones, Facebook, etc.—have far different attitudes toward technology than do older generations. There are now two distinct generations of digital natives in the United States: millennials (born 1979–1998) and Gen Z (born 1999 and after). The technology behaviors of these groups will affect adoption of technologies that impact family and home life in coming years, as more millennials become parents and as members of Gen Z hit their tween (10–12) and teen years.
- **Shifting demography.** Delayed marriage and parenthood is shrinking family size. At the same time, the strong connection between millennials and their baby-boomer parents has led to a rise in multigenerational households in the United States, a trend that has been further intensified by the Great Recession. The changes in the form and function of the home will happen within the larger context of these continued demographic shifts.