**IN THIS ISSUE** CYBERSECURITY FRAMEWORK • VOTING SYSTEM GUIDELINES • AI

# THE SciTech LAWYER

VOLUME 14 ISSUE 3 | SPRING 2018 | SECTION OF SCIENCE & TECHNOLOGY LAW | AMERICAN BAR ASSOCIATION

## POLICY CHALLENGES FACING CYBERSECURITY IN THE IoT AND BEYOND

MICHAEL A. AISENBERG AND PETER MCLAUGHLIN, ISSUE EDITORS

BY ROBERT S. METZGER

# SECURITY AND THE INTERNET OF THINGS

## The Role of the Federal Government to Reconcile Opportunity and Risk

The Internet of Things (IoT) is upon us. In fact, it is all around us. We may not know it, we do not own it, and rarely do we control it. But we are becoming dependent upon it, and therefore vulnerable to it.

Various forecasts indicate an astonishing growth rate and a staggering market size for the IoT. A *Business Insider* report from January 2017 estimates that by 2021, there will be 22.5 billion connected IoT devices—up from 6.6 billion in 2016—with the IoT sector seeing an expected $4.8 trillion in aggregate investment in that time. Bain & Company, in a 2016 report, estimated that by 2020, annual revenues could exceed $450 billion for IoT vendors selling the hardware, software, and comprehensive solutions that will make up the IoT. The federal government is a significant IoT customer already and its participation will grow. In December 2017, *Federal Computer Week* reported that an analysis by the Govini firm found the federal government spent nearly $9 billion in 2015 on sensor-enabled IoT technologies. The Pentagon dominates present federal IoT spending, according to the same report. Many other sources predict increased utilization by civilian agencies. IoT devices are at use in transportation, health care, power generation and distribution, and in a wide variety of industrial applications, not to mention innumerable consumer-facing appliances.

The IoT presents enormous promise for governments at all levels. Sensor-informed networks can accelerate the government's responsiveness. Hyperscale data collection can support analytics, artificial intelligence (AI), and autonomy with potential to transform industrial functions and government operations. However, accompanying these opportunities are new threats and expanded vulnerabilities. The consequences of cyberattack on the IoT grow as the scale and reach of IoT devices and systems expand.[1]

This article concerns how the federal government should act to reconcile the opportunities and risks of the IoT. The challenge is to simultaneously *enable*, *protect*, and *respond*. The government should strive to *enable* and exploit the IoT where it can improve the government's delivery of services and improve our national defense. At the same time, the government must *protect* key functions, scarce assets, critical infrastructure, and military capabilities as these become dependent upon the IoT.[2] The threat environment is pervasive, dynamic, and long-term. Adversaries will attempt "cyber-physical" attacks on IoT systems—cyberattacks that have physical effects on connected equipment—and some will succeed. Thus, the government must have the knowledge and means to *respond* and recover from such attacks.

## Defining the IoT

There are many definitions of the "IoT" reflecting the diversity of applications, and no definition has emerged as a standard. In July 2016, the National Institute of Standards and Technology (NIST) released Special Publication (SP) 800-183 ("Networks of 'Things'"), which observed that the "IoT involves sensing, computing, communication, and actuation." NIST distinguishes between the IoT, which is "tethered to the Internet," and the Network of Things (NoT), which could be a local area network (LAN) with none of its "things" connected to the Internet. NIST refers to "distributed systems" that employ IoT technologies, and defines a "distributed system" as "a software system in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal." NIST considers the IoT to be one type of a NoT and a NoT to be one type of a distributed system. Here, the discussion of "IoT" will encompass distributed systems that employ sensor-enabled networks which communicate both to and from hosts and with other sensors and which actuate devices at the network edge.

***Robert S. Metzger*** *(rmetzger@rjo.com) is a shareholder of Rogers Joseph O'Donnell, PC, a law firm that has specialized in public contracts for more than 35 years. He heads the firm's Washington office and counsels leading U.S. and international technology firms in cyber and supply chain security and in other areas of regulatory compliance and public policy.*

## The IoT and Defense Logistics

The IoT already figures into U.S. military capability and will acquire increasing importance. It will affect defense business systems, weapon systems, information systems, and operationally critical support. For example, the efficiency and responsiveness of military logistics can be greatly improved through IoT-enabled systems. The IoT can enhance the military's ability to transport equipment and deploy and support forces. It will affect both commercial and defense-specific logistics, as well as maintenance, repair, and overhaul. The IoT will produce better information about the hardware status—location, condition, disposition, availability, etc.—facilitating informed "asset liquidity." Planners and commanders will benefit in having greater knowledge of asset disposition and higher confidence of availability and readiness. Many decisions, ranging from the "home front" to the "tactical edge," and reaching from the logistics supply chain to commanders in the field, will be better informed and executed faster. In an era of expensive (and often scarce) capital assets, great advantage can be realized through timely maintenance, efficient sustainment, expedited asset movement, and higher assurance of availability and readiness. Serious dangers accompany these advantages, however. As the Department of Defense (DoD) comes to rely on an IoT-enabled supply chain and logistics operation, cyber-physical attacks on such systems could "blind" or disable support personnel, mission planners, and field commanders alike. Cyber-physical attacks on defense systems, including advanced manufacturing facilities, can have highly destructive effects.

## Cyber-Physical Threats

IoT systems commonly utilize information that is collected by sensors, transmitted within and among networks, and processed to generate information or command actions by connected systems. Cyber systems using IoT-connected sensors monitor, control, and operate physical systems. Cyber-physical threats are present where IoT networks, at any point, are vulnerable to intrusion or corruption that produces adverse physical effects on connected equipment. Once inserted, malware can exploit an "attack chain" until it reaches its intended targets. Cyber-physical threats include tainted firmware to introduce unwanted functions, subvert system integrity, or deny system access. Malicious code may be inserted into a software update of a distributed system. Cyber-physical threats can be very difficult to detect. They can be designed-in at inception, should the adversary have control or access to the supply chain at early stages, or they can be introduced later in the product life cycle, during the support or sustainment phase.

The IoT will include many new virtual and physical systems. These expand and create new attack surfaces and increase the vulnerabilities of present ("legacy") systems connected to IoT devices or controllers. The consequence of cyber-physical attacks is illustrated by the "Stuxnet" virus attack on Iran's nuclear enrichment facilities. Discovered in 2010, the Stuxnet attack subverted the control functions of gas centrifuges, causing them to self-destruct in operation. A very recent example is the "Trisis" attack on oil and gas facilities in the Middle East. Publicly revealed in late 2017, the attack involves a sophisticated computer virus specially engineered to sabotage industrial control systems used in factories and refineries. The breadth of potential IoT attacks is shown by the Mirai botnet attack of late 2016. The US-CERT unit of the Department of Homeland Security (DHS) issued an alert on October 14, 2017, which stated: "Recently, IoT devices have been used to create large-scale botnets—networks of devices infected with self-propagating malware—that can execute crippling distributed denial-of-service (DDoS) attacks. IoT devices are particularly susceptible to malware, so protecting these devices and connected hardware is critical to protect systems and networks." A research paper presented at the USENIX security symposium in August 2017 states that the Mirai botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady state population of 200,000–300,000 infections.

## New Vulnerabilities

The IoT operates by connection of end-point devices (e.g., sensor networks) to control systems and by communication along the edge as well as to the core. As seen by adversaries, attack surfaces will multiply, to include end-point devices, network interconnections, transport infrastructure, aggregation points, and control systems. Authentication, identity management, and transaction processing, which may be cloud-delivered, add to exposed surfaces. System-directed attacks may exploit insecure web connections. Attacks could be directed to core (client) functions, such as data analytics, which act upon received sensor data to generate instruction. Or, as illustrated by the Mirai botnets, attacks may be directed at the periphery, exploiting unsecure sensors of consumer or industrial devices to create a migration path for malware to infect and spread among core systems across multiple, targeted business sectors.

The IoT is exposed to a dangerous paradigm of "attack once; affect many." IoT networks involve massive interconnectivity and constant interdependence among devices, communications, and control. Where devices and dependent systems possess common vulnerabilities, single entry point attacks can circulate and cascade to impact numerous connected or codependent systems. One IoT attack could degrade or disable many power generators across an entire grid. Conceivably, IoT attacks could "poison" logistics and transportation systems, leaving managers without knowledge of equipment availability and readiness. Similar risks are posed to IoT-enabled manufacturing systems. An attack on unprotected IoT elements of a sensor-driven system could degrade command and control and compromise mission performance of advanced military systems.

## The Challenge for the Government

The IoT represents the confluence of many rapidly changing technologies that produce "radically disruptive" changes to the status quo. Extremes of commercial opportunity are presented. National economies will vie to best exploit the IoT. Across many sectors, the IoT will create new markets, change business models, and bring new competition. Companies will rush to sell IoT systems and products. New entrants will abound. Exploitation

of the IoT—for consumer, industrial, and government markets—will be characterized by strong pressures to be "first to market" and to employ "least cost" strategies. These work against security objectives. Taking the time to understand cyber vulnerabilities, or spending the extra money to secure the supply chain, can put vendors behind the pace of customer adoption or behind the curve of acceptance and deployment. Security will be a concern of some, but an objective of only a few.

Where poorly designed or operated with indifference to security, IoT systems can produce great harm to the public interest. The risks of trusting "market driven" solutions will be unacceptable where dependency on the IoT creates serious risk to critical infrastructure or national security. Though governments have many reasons to adopt and promote the IoT, government influence is limited. The pace and diversity of IoT technologies argue against a prescriptive regulatory approach, and political resistance to broad regulatory measures would be difficult if not impossible to overcome.

Resolving these tensions is a challenge of extraordinary complexity and importance. Critical infrastructure will become vulnerable to IoT cyber-physical attacks as private industry adopts the IoT for its own purposes, independent of government participation or knowledge. The government may be "along for the ride," so to speak, with little awareness or control over how it is affected by the IoT. Needless to say, this situation anticipates "learning the lesson" of prophylactic IoT security only after one or more attacks produce harmful, perhaps calamitous, effects. The challenge is how to manage government intervention to address IoT threats to critical infrastructure and national defense, while not stifling innovation or denying the government the benefit of IoT functionality.

## How the Government Can Act

At any given time, the government may act as sponsor, purchaser, regulator, consumer, protector, or responder. Risk management considerations argue for government initiatives to be informed, at least, where the IoT affects critical infrastructure or key national defense functions. Without knowledge, the government cannot defend its assets and preserve national capabilities. Informed, the government can choose to encourage, or if necessary compel, the private sector to take positive measures to improve security. A risk-informed, selective approach is necessary.

The government is not without power to affect the IoT and protect against its risks. It has *legislative* power to enact laws.[3] Agencies can use their *regulatory* authority to mandate practices within or among sectors. As *purchaser*, the government can fund programs to develop technical measures to answer or recover from IoT threats. The government has unique sources and types of *information* that it can use to inform industry of threats and recommend responses. It can bring *enforcement* actions against individuals or companies that violate laws or regulations concerning IoT security. When it funds research or purchases supplies and services, the government can use its *acquisition* authority for many relevant purposes. Actions to consider include the following:

- Enact legislation to unify federal responsibilities for IoT defense and recovery;
- Fund programs and technology development to improve IoT security;
- Sponsor research to apply best commercial technologies to IoT defense;
- Assess supplier IoT security for contract eligibility and in source selection;
- Fund systems security engineering, IoT risk assessment, testing, and response;
- Establish standard federal frameworks for IoT risk management and IoT security;
- Encourage or require contractor use of standards and best practices;
- Require agencies and contractors to assess and test for IoT vulnerabilities;
- Harden systems vulnerable to IoT attack and implement fail-over mechanisms;
- Obligate contractors to assess and disclose IoT use for high-impact systems;
- Encourage federal contractors to rely on trusted suppliers;
- Facilitate reporting of IoT exploits and establish safe harbors for data sharing;
- Apply AI to event reports and automate dissemination of event information;
- Periodic exercises to test response to and recovery from IoT attacks; and
- Legal action against companies that fail to satisfy IoT security obligations.

These are suggested ways for the federal government to address IoT risks. Many constructive actions are possible without statutory action—though enactment of the Warner-Gardner bill, or legislation along its lines, would be helpful. If IoT security is to be generally required of federal contractors, formal rulemaking may be required. This gives all stakeholders an opportunity to participate, but it is a slow process. Delay is not an ally of security considering the speed of IoT adoption. Agencies may determine that some IoT threats require more immediate response. Hence, for individual contracts, federal agencies may be justified in establishing minimum qualifications (for bidders) and special contract requirements, to address IoT security risks and respond to IoT attack events. For critical functions, agencies may need to assess contractors for supply chain risk and require planned measures to harden systems and recover from attacks.

## Lessons from the DSB Cyber Supply Chain Report

In April 2017, the Defense Science Board (DSB) released a cyber supply chain report.[4] The DSB task force was to "assess whether current practices are able to effectively mitigate malicious supply chain risk." The focus of the report was on how key defense systems are exposed to threats to the functionality and reliability of electronic systems, threats that

*Continued on page 13*

# Security and the Internet of Things

*Continued from page 7*

can be mounted by attacks on the supply chain for such systems. Most defense systems utilize electronic parts and computing systems that depend on such parts. One vulnerability is to counterfeit electronics where the part acquired or used is not as represented and may fail when use is attempted in the intended environment. Another vulnerability is that adversaries may insert malicious code into electronic parts during their design or fabrication. Likewise, weaknesses in firmware or software expose electronic parts and systems to subversion by insertion of malicious code after installation.

The report was not written with the IoT as a focus. However, findings and recommendations of the report are relevant to assessment and response of IoT cyber-physical vulnerabilities. Specifically, the DSB report illustrates many attack vectors and potential consequences should adversaries exploit hardware, software, or system vulnerabilities in IoT-enabled systems. Among the key findings:

- The existence of counterfeit electronics in the supply chain demonstrates the potential for attacks that involve malicious insertion of compromised electronic parts. Malicious insertion may be very difficult to detect.
- Reporting requirements for counterfeit parts are inconsistent and the existing system for reporting nonconforming or counterfeit parts is antiquated. No system now collects event information on cyber-physical attacks. Means are needed to rapidly process and act on alerts and disseminate vulnerabilities and response.
- Supply chain penetration can be achieved through internal or external threats, as a result of latent vulnerabilities or poor design, or by active exploitation. Sustainment is particularly susceptible to supply chain attacks.
- The DoD now requires suppliers to protect the confidentiality of controlled technical information. Today's cyber Defense Federal Acquisition Regulation Supplement (DFARS) protects information and information systems against exfiltration but does not now address the distinct software or firmware cyber-physical threat to parts and systems.

A number of the DSB report observations express principles that can be applied by government agencies, program sponsors, and other officials to manage and respond to IoT threats. *Reducing supply chain vulnerability* can be done by protecting design, supply chain, manufacturing, and distribution systems; employing better assurance; and utilizing diverse design with built-in active monitoring and surveillance, with rapid upgrade capability. The report advocates *preparation* by DoD activities, to identify vulnerabilities, detect exploitation, respond, and recover (restore system to trusted state).

## Conclusion

National advantage can be obtained through the government's sponsorship and use of IoT technologies. But the IoT faces new threats and creates new vulnerabilities. Because of the scale of systems potentially dependent upon IoT elements that share common or single-point vulnerabilities, successful IoT attacks could cripple vital national capabilities or compromise government ability to plan and act. Hence, security must be given greater priority. Defense of the IoT will be formidably difficult. While hardening against attacks is demanding enough, IoT systems important to national defense or critical infrastructure must be made survivable, so that they can operate while under attack, and resilient, so that systems recover quickly after attack. Automated means to detect and classify threats, and to execute subnetwork isolation, should be pursued. Industry and government are committed to the huge IoT market opportunity. Security must be given greater, if not equal, priority. Securing against cyber-physical threats to the IoT will not be achieved by a passive government posture or reactive industry measures. The government should use the tools available to it, as a national priority, for security of the IoT. ◆

## Endnotes

1. Also to consider, though outside the scope of this article, are risks posed by the IoT to privacy. IoT sensors acquire, accumulate, and process truly massive amounts of personal data.

2. The Department of Homeland Security has identified 16 critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. All will be affected by IoT technologies.

3. Presently before Congress is the proposed "Warner-Gardner" legislation, formally the "Internet of Things (IoT) Cybersecurity Improvement Act." The legislation, if enacted, would impose minimum cyber hygiene requirements on federal purchases of Internet-connected devices. Agencies would be required to include in provisions that require contractor certification that the devices they sell (1) contain no known security vulnerability or defect; (2) rely on software or firmware that can be updated from trusted sources; (3) use industry-standard protocols for communication, encryption, and interconnection; and (4) do not include any fixed or hard-coded credentials for remote administration. The Act also would require contractors to notify the purchasing agency of any known security vulnerabilities.

4. The author was a member of the DSB task force that produced the report. The views expressed in this article are personal to the author and should not be attributed to the Department of Defense, to the Defense Science Board, or to any client or other organization with which the author is affiliated.