The Implications of IoT for Cyber Conflict

By LTC BE Rhodes, Colorado Army National Guard

"The number and type of attacks, the duration, the scale, and the complexity of these attacks are all on the rise." – Kyle York, Chief Strategy Officer, Oracle Dyn

There are many dates in history that people remember exactly where they were due to the significance of the event, such as John Kennedy's assassination or the Space Shuttle Challenger accident. On October 21, 2016, many users across the United States remember they were unable to reach some of the biggest names of the Internet era: Amazon, Netflix and Twitter. Beginning mid-day the largest ever distributed denial of service (DDoS) attack was conducted against Domain Name Services (DNS) and infrastructure provider Dyn. With an estimated throughput of 1.2 terabytes, the Dyn team was able to identify more than 100,000 devices that were now part of the infamous Mirai botnet that were sending malicious traffic to their distributed points of presence (for the company's enterprise DNS services) on the East Coast (Figure 1). What made the Mirai botnet so concerning was the use of easily exploited Internet of Things (IoT) devices including closed-circuit television (CCTV) cameras with hard-coded username/password combinations. The Dyn attack should have been a wake-up call for the IoT industry, slowing the pace of development to better assess security. If anything, the numbers of devices that are now considered IoT has increased exponentially. Cyber warfare planners must now account for these devices or risk unforeseen consequences.

They found that a mere one-percent bump in electric consumption by high-demand IoT appliances (for example, air conditioners) in the right geographic location could cause a power outage for millions of people.

The term IoT has become synonymous with the idea that any device can (and some would argue should) be connected to the Internet. There are many example devices which the general consumer are very familiar: smart phones, smart speakers, streaming entertainment boxes, smart televisions, thermostats, and security cameras. More recent additions to IoT include deadbolts, crockpots, refrigerators, water heaters, cooktops, baby monitors, light bulbs, garage door openers, cars, and the list goes on. Farmers are even putting IoT sensors on cows to manage the health of their herds!

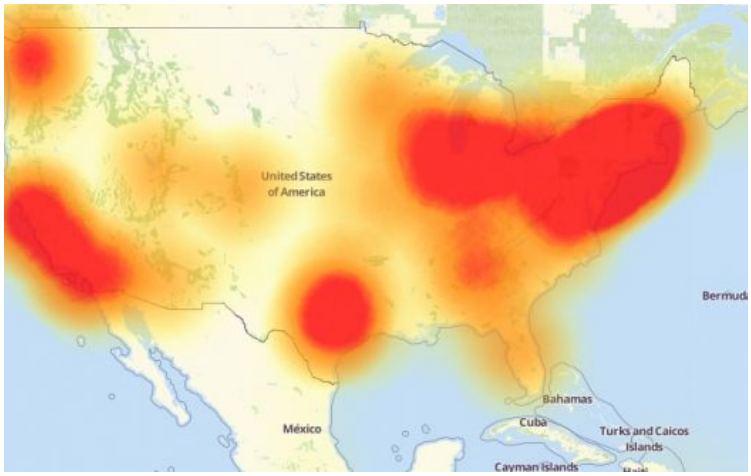

Figure 1
downdetector.com via
https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/

Many of these devices are sold to consumers, who had little to no knowledge of the complexity of the actual technology, on the basis of convenience. All they have to do is connect the many devices to a WiFi access point and they can now manage their "smart home" from afar, seemingly trusting companies with the data about their homes and lives with little care. Viewed in the larger context of "smart cities" (Figure 2), the risks of another Mirai-type botnet should be considered a real possibility.

Princeton University researchers recently published a study that seems to confirm the reality of such a risk. They found that a mere one-percent bump in electric consumption by high-demand IoT appliances (for example, air conditioners) in the right geographic location could cause a power outage for millions of people. As more is asked of the electric grid, US energy providers are already looking for ways to reduce usage at peak times. For example, Xcel Energy is offering a "Saver's Switch" where customers can cede control of their central air conditioning on hot days to benefit the entire grid. This means that a persistent threat actor only has to gain access to Xcel Energy's central control to create

the effect studied at Princeton. Consider that the majority of the United States military bases are dependent on the same utilities as those potentially susceptible to an IoT-generated cyber attack and the impact on real operations could be severe.

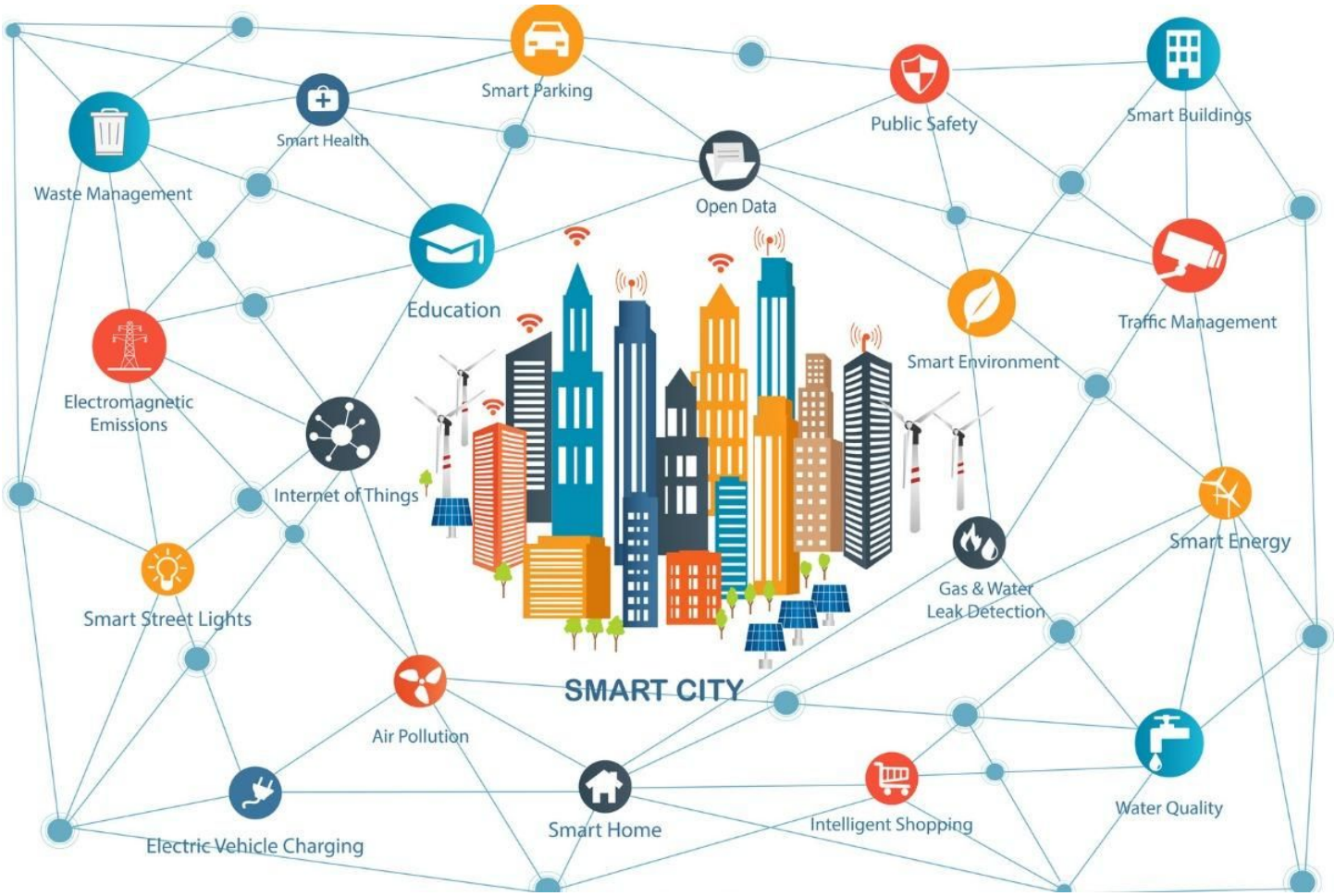

Figure 2
https://www.smartcitiesworld.net/news/news/smart-cities-services-worth-225bn-by-2026-1618

The first challenge is the scale of the problem. In 2017, Gartner predicted that by 2020 more than 20 billion devices (billions of which can be considered IoT) will be connected to the Internet. For a time, many industry leaders in the field referred to IoT as the "Internet of Everything", which is becoming a more accurate description daily as all of these devices have an operating system with TCP/UDP ports exposed on the network to function. While many sit behind a NAT, firewall, or other network perimeter protection, there is a sizeable number that do not (simply look at Shodan - https://www.shodan.io/). As the Mirai botnet proved threat actors are happy to use whatever they find exposed, and it only takes one vulnerable thing to impact an organization's bottom line. In short, military cyber planners have to consider each unique surface of every IoT device family inside their networks and the potential vectors they provide for an adversary. It is much easier for an attacker to hide in billions of devices than the several thousand found on a typical corporate network.

Cyber planners and commanders must now account for every device in use by service members and third parties in and around their operational locations.

The next challenge is the IoT supply chain. Since manufacturing is much less expensive overseas, the components of most IoT devices or entire devices are

imported to the United States. This is problematic in cyber conflict because there is little trust, if any, that the supply chain is not already compromised by one or more state actors. This concern was highlighted in October 2018 by Bloomberg's exposee of the alleged compromise of Supermicro boards via firmware. When the supply chain is suspect, the entire system is at risk. Military cyber planners now have to be concerned whether or not the IoT medicine dispenser is compromised and service members die due to incorrect dosages, not from enemy fire.

Another challenge facing cyber planners is asset management. This boils down to knowing what is actually on hand and what users bring with them. Many organizations purchase and place technology on the network where it remains in operation for years, eventually to be forgotten. As those devices become outdated, they become vulnerable to easy exploitation. Couple that with the more recent concept of bring your own device (BYOD), where employees can use their own laptops, tablet, smartphones, or smart speakers to access organization infrastructure, and security professionals have increasing blind spots throughout their networks. It is difficult to defend the unknown, and threat actors know that. Finally, cyber planners are tested by the human element. Humans buy tech to make their lives better. They blindly agree to end user license agreements that give away their data and metadata to a money-making enterprise that may or may not actually use the information. Worse, IoT-derived data can directly risk the lives of service members in harm's way. Case in point, in November 2017 Strava (a social network for athletes) released activity mapping data from millions of fitness wearables check-ins. While an interesting case study of human activity, it potentially revealed the location of sensitive US military locations around the globe (Figure 3). Not one service member signed up to violate operations security (OPSEC) when they started using a seemingly-harmless IoT device, but they did. Cyber planners and commanders must now account for every device in use by service members and third parties in and around their operational locations.

Figure 3
https://twitter.com/Nrg8000/status/957318498102865920

As IoT devices continue to proliferate, they provide with a rich set of vectors (how access is gained on systems) for potential attackers. When considering IoT, the sheer volume makes it nearly impossible to catalog all of the surfaces (the total number of vectors available in a given environment) that could be exposed. Eventually, network connectivity requirements will not be optional for IoT devices, as they will not function without it. As smart grids continue to expand, even military bases will not be able to avoid allowing the integration of IoT power sensors to meet stricter energy use standards. Cyber planners must account for these facts because, on the flip-side, threat actors will as well. The endgame for any threat actor is to gain access to an enterprise. They do not care if they get in via a phishing email or through an "accidentally" exposed interface on a security camera, HVAC system, or VOIP phone. As the maxim goes, threat actors only have to be right once, while defenders have to be right every time.

In December 2017, the co-creators of the Mirai botnet - Paras Jha (from New Jersey) and Josiah White (from Pennsylvania) - plead guilty to their scheme. As described by journalist Brian Krebs (one of Mirai's first victims), Jha and White can be likened to firefighters starting fires intentionally and then putting them out as heroes. By taking advantage of easily exploited flaws in IoT devices, Jha and White wreaked havoc on the whole Internet. In the aftermath of Mirai, the implications of IoT for

cyber conflict are quite clear. Threat actors no longer need to access high-end network or system assets; they just need someone in an organization to utilize and expose a vulnerable IoT device.

Cyber defense planners in both military and commercial spaces must address exponentially expanding threats and vectors created by IoT. There are multiple areas of concern (not all inclusive): the growth in the number of IoT devices (which can be just about anything) is accelerating daily; IoT devices have proven they can and do create OPSEC risks; large facilities such as military bases will have no choice but to become more integrated with smart grids in the communities where they reside; supply chain safety for all technological devices is considered suspect (who knows if the replace part has a chip that will open a backdoor or fail at a pre-planned time); and finally, the growing reliance on IoT in the civilian and military sectors will reach a point where workplace integration becomes inevitable. IoT assets must now be accounted for cyber defense plans or planners risk their organizations becoming the next victim in a contested domain that grows more complex every day.

LTC BE Rhodes is a Cyber Warfare Officer in the Colorado Army National Guard where he commands Cyber Protection Team 174. He holds multiple professional certifications, regularly speaks on cyber

defense and incident response, and teaches at the graduate-level. LTC Rhodes enjoys building with Raspberry Pi and Arduino IoT devices to model SCADA/ICS to demonstrate kinetic-cyber effects for senior leaders. He has drowned countless Lego people over the years and helped many understand that connecting to unsecure WiFi is a terrible idea! You can find him on LinkedIn and Twitter (@cyber514).

---

1. York, Kyle. “Dyn’s Statement on the 10/21/2016 DNS DDoS Attack”, Dyn Blog, https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ (October 21, 2016)
2. Roberts, Jeff J. “Who to Blame for the Attack on the Internet”, Fortune, http://fortune.com/2016/10/23/internet-attack-perpetrator/ (October 23, 2016)
3. Hilton, Scott. “Dyn Analysis Summary Of Friday October 21 Attack”, Dyn Blog, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (October 26, 2016)
4. Frulinger, Josh. “The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet”, CSO (from IDG), https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (March 9, 2018)
5. Fildes, Nic. “Meet the ‘connected cow’”, Financial Times, https://www.ft.com/content/2db7e742-7204-11e7-93ff-99f383b09ff9 (October 25, 2017)
6. Greenberg, Andy. “How Hacked Water Heaters Could Trigger Mass Blackouts”, Wired, https://www.wired.com/story/water-heaters-power-grid-hack-blackout/ (August 13, 2018)
7. “Saver’s Switch: Residential”, https://www.xcelenergy.com/programs_and_rebates/residential_programs_and_rebates/home_energy_efficiency/savers_switch
8. Tung, Liam. “IoT devices will outnumber the world's population this year for the first time”, ZDNet, https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/ (February 7, 2017)
9. Varinsky, Dana. “Here's what 5 of your favorite products would cost if they were made in the US”, Business Insider, https://www.businessinsider.com/how-much-products-would-cost-if-made-in-us-2016-11 (November 27, 2016)
10. Riley, Michael and Robertson, Jordan. “The Big Hack: The Software Side of China’s Supply Chain Attack”, Bloomberg, https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-the-software-side-of-china-s-supply-chain-attack (October 4, 2018)
11. Hsu, Jeremy. “The Strava Heat Map and the End of Secrets”, Wired, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ (January 29, 2018)
12. Krebs, Brian. “Mirai IoT Botnet Co-Authors Plead Guilty”, Krebs on Security, https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/ (December 13, 2017)