Killer Thermostats: Countering the Internet of Terrorism (IoT)

Co-Authored by Col. Patrick M. Duggan Commander, Joint Base Myer-Henderson Hall

Col. Patrick M. Duggan

Should you be scared of your new thermostat? Maybe, if it is WIFI-enabled and you haven't secured it.

Why? The next generation of terrorism is here, and it will use your connected devices – thermostats, fridges, lights, elevators, industrial controls, cars – even toys. These smart devices represent the latest pathways for tech-savvy terrorists to wreak chaos. But before unplugging everything you own to live off the grid, take heart in the fact, at least at the national level, we still have time to prepare.

While traditional DoD counter-terrorism (CT) efforts have mainly emphasized direct action, future U.S. security measures must also adapt to harness the Internet of Things (IoT). Simply put, the IoT's inexorable growth portends new methods for destruction but also provides new mechanisms for defense.

These same IoT devices are as capable for U.S. Special Operations Forces (SOF) hunting terrorists as they are to the enemies who use them. This phenomena of unconventional cyberwarfare will become increasingly critical to defending the nation and heralds the birth of a new form of CT: countering the Internet of Terrorism (IoT).

The concept of "edge computing" is breeding entirely new ecosystems – and terrorist threats. Edge computing is a critical driving force behind IoT's ever-expanding adaption to new fields of computer application. Instead of a centralized hub to process data or information, edge computing enables virtually anything with a mini-processor to use its own "smarts" to respond at the very source of the data. This capability means that end-user client devices can carry out a multitude of nefarious activities independently or as part of a more coordinated "foggy network."

According to leading reports, by 2025 a huge percentage of the devices we use regularly in our daily life will be connected; and our wearables, ingestibles, sensors, transportation systems and devices will all become a node on constantly emitting and transmitting networks. Not only will this explosion of technology drive privacy issues and self-determined freedom over our individual lives, but it can kill us as well.

Take for example, the fact that the Islamic State in Iraq and Syria (ISIS) is already employing off-the-shelf drones to drop bombs and fly kamikaze-like missions into U.S. and Iraqi SOF partners in Northern Iraq. How much longer will it take for the next "terror-byte" step, to use edge computing technology so that a terrorist can build his own swarm of killer drones in a garage?

And making it even harder to counter, the garage can be a thousand miles away, with units operated like some sort of macabre video game.

How will Soldiers destroy a swarm of bomb-laden drones coming at them from multiple directions when they are moving on the ground? The answer is to use a defensive structure that is as flexible and adaptive as the enemy. The best protection requires leveraging our own network of miniaturized and remote systems to create a counter-swarm!

Special Operations and Cyber operations can work together effectively to provide low-cost, high effectiveness defense against a number of newly emerging terrorist threats. There are clearly big-data threats that require big-computer systems to defend against – exactly the type of capabilities developed by U.S. Cyber Command (CYBERCOM). Many threats, however, are both more tactical and more distributed. In order to defend against these dangers, it is necessary to have counter-capabilities that are also tactical and locally disseminated.

We encourage the creation of a new Special Operations Command-Cyber (SOC-CYBER). Similar to the Theater Special Operations Commands (TSOCs) every Geographic Combatant Commands owns, SOC-CYBER would provide the same integration, synchronization and oversight of better fused cyber-SOF missions.

Co-locating some of the nation's most talented warriors with those trained to counter emerging technical threats would help ensure America stays ahead of the coming Internet of Terror.

But still, don't forget to add a password to your thermostat.

Editor's note: Duggan's co-author is Scott S. Gartner, Director of Pennsylvania State School of International Affairs. Reprinted by permission, this article first appeared in the Huffington Post March 3, 2017.

PCBs: Cleaning up the former 'miracle chemical'

By Jen Tolbert Environmental Management Division, JBM-HH Directorate of Public Works

A substance that has low flammability, chemical stability, and excellent insulating properties and could come in the form of liquid oil or a waxy solid – this was every industrial and commercial manufacturer's dream chemical.

Because of these valuable properties, polychlorinated biphenyls (PCBs) were used in a wide variety of products including transformers, capacitors, pesticides, paints, adhesives, plastics and many more.

PCBs were manufactured from 1929 until 1979, when production was banned due to negative human health and environmental impacts. While PCBs are no longer manufactured, and many PCB-containing products have been taken out of use, they can still be released into the environment from improper maintenance and disposal of older PCB products.

Poorly managed hazardous waste sites, illegal dumping, disposal of PCB-containing products at landfills not designed to handle hazardous waste, burning of PCB waste in incinerators and leaks from PCB-containing transformers have all been causes of PCB releases to the environment.

States in the Chesapeake Bay area are working to reduce PCB contamination in the Bay by establishing new regulations and requirements to prevent PCBs from entering waterways.

In 2007, Virginia, Maryland, and the District of Columbia, developed Total Maximum Daily Loads (TMDLs) for PCBs for tidal portions of the Potomac and Anacostia Rivers. These TMDLs establish amounts of PCBs that a waterbody can receive while still meeting required water quality standards and allow states to place restrictions on facilities with the potential to discharge stormwater to the Bay.

These facilities are often required to develop PCB TMDL Action Plans to identify any potential sources of PCBs and plan how to ensure they do not pollute waterways.

Even though Fort Myer and Henderson Hall do not discharge directly to the Bay or the Potomac River, the Environmental Management Division recently developed a PCB TMDL Action Plan for Fort Myer and Henderson Hall, as a requirement for the Installation's Virginia Municipal Separate Storm Sewer System (MS4) Permit. Because Fort McNair is not located in Virginia and does not have the same requirements, it was not included in the action plan.

COURTESY PHOTO

The Potomac River is covered under the Total Maximum Daily Load (TMDL) for polychlorinated biphenyls (PCBs).

The purpose of the action plan is to identify potential sources of PCBs on the base and ensure the public and environment are protected from the effects of PCBs.

No significant sources of PCBs were identified at Joint Base Myer-Henderson Hall through the research conducted for this action plan. Historically, the main potential sources of PCBs on JBM-HH have been transformers. However, all pure PCB transformers have been removed from the installation or retrofitted with mineral oil to prevent adverse environmental and human health impacts should a transformer leak oil.

Fluorescent light ballasts are another historical source of PCBs on base. After the manufacture of PCB-containing light ballasts was banned by EPA in 1979, existing PCB-containing fixtures on the installation were gradually replaced. If old fluorescent light ballasts are discovered, they are replaced.

The PCB ballasts, which contain only a very small amount of PCBs, are properly managed and disposed. In fact, all hazardous waste is effectively managed on base to protect people and the environment and ensure harmful substances, including PCBs, are properly contained and disposed.

To report conditions that could cause stormwater pollution or to get more involved with stormwater activities at JBM-HH, call the Environmental Management Division at 703-696-8055.

For more information and guidance resources on PCBs, visit EPA's PCB webpage (www.epa.gov/pcbs).

PAO recognized in Army-wide competition

By Public Affairs Office Staff

We would like to take a small space (we want to keep to telling, not being the news) here to give praise to one of our own (okay, we're patting ourselves on the back).

Emily Myers, public affairs specialist, first served a developmental assignment with JBM-HH PAO in 2016; then, we were fortunate to hire her away from Aberdeen Proving Ground, Maryland, in January.

Bottom line: Annual Keith L. Ware Journalism awards were distributed in late February, and we are proud to note that Ms. Myers – our EM – is on a team of five at Aberdeen Proving Ground who won first place in Installation Management Command's Community Relations category for "Community Leader Engagements."

Myers' job on the APG team was filming social media videos and broadcasting various community augmentation events between civilian community and base leaders, enhancing partnership opportunities on and off APG: school systems, housing partners, municipal and state government partners. She did her part to explore issues that are important to military and civilian neighbors divided by a fence and helped foster relationships and share solutions. This IMCOM first place has been forwarded on to Department of Army.

She brought her talent and expertise with her from APG, and we are proud to say that Myers won an individual award in Social Media Video at JBM-HH for her video "See Something, Say Something."

Always topical, see it at https://www.facebook.com/jbmhh/videos/10154621001902074/.

Contact Myers in the Fusion Cell, Building 59, room 219, Fort Myer, emily.n.myers.civ@mail.mil or 703-696-8897.

PHOTO BY FRANCIS CHUNG

Public affairs specialist Emily Myers poses outside of Joint Base Myer-Henderson Hall Headquarters March 7.

Stay connected! www.army.mil/jbmhh Facebook: Facebook.com/jbmhh Flickr: Flickr.com/photos/jbm-hh Twitter: @jbmhh Slideshare: slideshare.net/jbmhh

Pentagram

703-696-5401

The Pentagram is an authorized publication for members of the Department of Defense. Contents of the Pentagram are not necessarily the official views of the U.S. Government, the Department of Defense, the Department of the Army, Department of the Navy, or Joint Base Myer-Henderson Hall. The content of this publication is the responsibility of the Joint Base Myer-Henderson Hall Public Affairs Office. Pictures not otherwise credited are U.S. Army photographs. News items should be submitted to the Pentagram, 204 Lee Ave., Bldg. 59, Fort Myer, VA 22211-1199. They may also be e-mailed to sharon.e.walker.civ@mail.mil. The Pentagram is printed by offset every Thursday as a civilian enterprise newspaper by APG Media of Chesapeake, LLC. APG Media of Chesapeake, LLC is located at 29088 Airpark Drive, Easton, MD 21601. Telephone (301) 921-2800. Commercial advertising should be placed with the printer. APG Media of Chesapeake, LLC Publications is a private firm in no way connected with the Department of the Army or Department of the Navy. The appearance of advertisements in this publication, to include all inserts and supplements, does not constitute an endorsement by the Department of the Army or Department of the Navy of the products or services advertised. Everything advertised in this publication shall be made available for purchase, use, or patronage without regard to race, color, religion, sex, national origin, age, marital status, physical handicap, political affiliation, or any other non-merit factor of the purchaser, user or patron. A confirmed violation of this policy of equal opportunity by an advertiser shall result in the refusal to print advertising from that source.

Col. Patrick M. Duggan Commander

Command Sgt. Maj. Carolyn Y. Donaldson Command Sergeant Major

Michael L. Howard Public Affairs Director

Sharon Walker Command Information Officer

Brent S. Wucher Editor brent.s.wucher.civ@mail.mil

Matthew Getz Graphic Designer

Delonte Harrod Staff Writer dharrod@dcmilitary.com

Julia LeDoux Staff Writer jledoux@dcmilitary.com

Arthur Mondale Staff Writer awright@dcmilitary.com

Jim Dresbach Staff Writer jdresbach@dcmilitary.com

Francis Chung Staff Photographer fchung@dcmilitary.com