Risks Associated with the Internet of Things

Overview
The Internet of Things (IoT) is a network of internet-connected objects able to collect and exchange data using embedded sensors [1]. The IoT is a relatively recent and lesser-known component of infrastructure. While a substantial increase of internet-connected devices is a promising prospect for industry (particularly the transportation, healthcare, defense, and information technology sectors), it creates unique opportunities for non-state or state actors to inflict economic and physical harm on the United States. The risk is found in the remote manipulation of infrastructure elements and consumer goods with internet connectivity (cars, phones, houses, utilities, etc.). This problem is not only relegated to the private sector, as the IoT is creating increased vulnerability for Department of Defense facilities, equipment, and employees—all of which are becoming interdependent through heightened internet connectivity [2].

Risks
Heightened connectivity is at the forefront of industry business practices and innovation. Security risks stemming from heightened connectivity are expected to grow [3,4] as the number of internet-connected devices is expected to reach 50 billion by 2020 [5]. Without robust security measures, the heightened connectivity of devices can be dangerous, as many of the technologies in the IoT could be exploited for nefarious purposes.

An example of the threat associated with the IoT is the automobile, a ubiquitous aspect of U.S. transportation infrastructure. The number of internet-connected vehicles is growing quickly, with more than 100 vehicle lines for 2017 equipped with this capability [6]. Internet-connected vehicles are vulnerable to remote exploitation, as was demonstrated in 2015 when white hat hackers manipulated the brakes, transmission, and steering of a Jeep on the highway [7]. The manipulation of a single vehicle on a densely populated highway is dangerous enough, but this risk could be compounded if multiple vehicles were compromised simultaneously in several widespread geographic areas, leading to a highly complex mass-casualty event. As the ability to hack into modern vehicles advances, the threat of cyberterrorists exploiting multiple vehicles simultaneously in a single event also increases. As with automobiles, software-controlled medical devices, like pacemakers, offer a bad actor the ability to directly target embedded, life-sustaining technology [8]. This specific scenario, in which a terrorist could disable life-sustaining technology, was a concern for high-level government officials during the Bush administration [9].

Mitigation
As is the case with any novel threat, the first and most crucial step in mitigation is awareness. Awareness of potential risks of the IoT is important for companies that manufacture and market devices with internet connectivity. Beyond awareness is the necessity of active mitigation measures. Investing in advanced cybersecurity tools, such as intrusion detection systems [10], security information and event management systems [11], and keyless signature infrastructure systems [12] may decrease the likelihood of bad actors utilizing device connectivity to orchestrate mass casualty attacks.

Summary
While the threat posed by a conventional terrorist attack (suicide bomb, active shooter, etc.) is still significant, the risk a bad actor takes in carrying out an attack is also significant. However, the risks a bad actor takes in exploiting the IoT is significantly lower than the risk associated with conventional terrorist attacks. This is because manipulating technologies connected to the IoT can be carried out remotely by utilizing systems already in place. Exploiting the IoT is accomplished using the connectivity of the financial services, transportation systems, and energy sectors as a weapon against their primary users. Attacks such as these will not only harm people but can also cause substantial damage to the economy and critical infrastructure components in the United States. Therefore, promoting awareness of these threats, along with developing mitigation techniques, is important for the defense and homeland security enterprises.
REFERENCES


ABOUT THIS PUBLICATION:
All information regarding non-federal, third party entities posted on the HDIAC website shall be considered informational, aimed to advance the Department of Defense (DoD) Information Analysis Center (IAC) objective of providing knowledge to the Government, academia, and private industry. Through these postings, HDIAC’s goal is to provide awareness of opportunities to interact and collaborate. The presence of non-federal, third party information does not constitute an endorsement by the United States DoD or HDIAC of any non-federal entity or event sponsored by a non-federal entity.

The appearance of external hyperlinks in this publication and reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or HDIAC. HDIAC is a DoD sponsored IAC, with policy oversight provided by the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)), and administratively managed by the Defense Technical Information Center (DTIC). For permission and restrictions on reprinting, please contact publications@hdiac.org. Any views or opinions expressed on this website do not represent those of HDIAC, DTIC, or the DoD.