This paper focuses on

- Changes in, or at least assumptions about, the cyber threat landscape
- Suggestions for rapid identification and analysis of emerging threats, and
- Considerations for managing and responding to future attacks

CYBER THREAT LANDSCAPE EVOLUTION

Some chilling, or depressing, thoughts to consider:

- Critical infrastructure attacks continue to be on the rise; we are living in a post-Ukraine era where we've witnessed the lights going out on hundreds of thousands of people. Numerous other control system attacks have been noted recently as well (German steel mill attacked 2014, Rye Brook, New York Dam Attack reported in 2016, petrochemical plant in Saudi Arabia August, 2017)[1].
- Growing attack surface especially in the global number of Internet of Thing (IoT) devices – counting both the consumer, and enterprise/B2B sides. Over 7 billion devices in 2018 expected to top 10 billion by 2020 and 22 billion by 2025[2].
- Organizations are increasingly at risk of supply chain compromise, whether intentional or unintentional. The factors that allow for low-cost, interoperability, rapid innovation, a variety of product features, and other benefits, also increase the risk of a compromise to the cyber-based supply chain, which may even result in risks to the end user[3]. Of significant concern for the United States is reliance on off-shore manufacture of integrated circuits. At year-end 2015, there were 94 advanced fabrication facilities in operation worldwide, of which 17 were in the United States, 71 in Asia (including 9 in China), and 6 in Europe. The Chinese government regards the development of a domestic, globally competitive semiconductor industry as a strategic priority with a stated goal of becoming self-sufficient in all areas of the semiconductor supply chain by 2030[4]. If we assume that the manufacture of integrated circuits is at risk, then a follow-on threat might be that devices coming out of the cardboard box have already been "pre-infected", or at least prepared to accept, malware sometime in the future.
- Again, assuming that the supply chain for integrated circuit manufacture has been compromised – this could lead to the evolution of cyber threats going

[1] Details on all of these cyber-attacks can be found at https://ics.sans.org
[2] Sourced from - https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[3] Sourced from - https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management
[4] Sourced from - https://fas.org/sgp/crs/misc/R44544.pdf

stealthy. By employing non-Internet based communication methods, leveraging portions of the RF spectrum [5] – either through *living off the land*, or using communication methods provided via a compromised supply chain – cyber threat actors might soon be by-passing traditional perimeter protection devices (firewalls, IDS systems, etc).

Rapid Identification & Analysis of Threats

Given the ever increasing volume and velocity of cyber threats, and the potential of malware operating in a stealthy manner, and the potential for *bad* AI to be directing the malware of the future – it is clear that the defenders will need to significantly speed up the process for developing a rapid situational awareness of cyber events/attacks taking place. Historically, cyber threat information sharing has been used on *final product* data – something that was presumed to be malicious with at least some level of confidence. Looking forward, it will become essential to use machine-machine information sharing techniques in ways to more rapidly progress along the anomalous – suspicious – malicious curve.

Managing / Responding against future cyber threats

The job of the defenders has always been difficult, but it seems to be getting harder and harder every day – especially if considered against supply chain compromise, and cyber threats operating with out-of-band communication capabilities. Imagine future scenarios where blocking traffic cannot be done in a firewall or in a BGP router – rather it might require blocking communication channels using the RF spectrum.

But first and foremost the defenders need to develop their trust communities, and methods to support machine-machine information sharing and the development of much more rapid situational awareness of anomalies detected within their enterprise.

Especially in the area of critical infrastructure, new methodologies will need to be developed to comprehensively confirm that systems have been *cleaned up* to allow systems to return to service – in both the IT and OT domains.

[5] Communication relay supplemented with the use of Unmanned Aerial Vehicles would greatly reduce the transmit power required.