CTC #15

This podcast is a part of a series of conversations with cybersecurity researchers and analysts who are actively tracking down threats in cyberspace. This particular episode released in June 2018, discusses the activity of a certain Chinese hacking group that is linked back to a Chinese government intelligence organization. Tom Hegel, the interviewee, is from the 401 Threat Research Group (401TRG), a team at ProtectWise analyzing network traffic, malware and much more. He discusses the historical and recent activities of “the Winnti Umbrella” a cyber threat group linked to Chinese intelligence organizations. The conversation is detailed and fascinating as well as presented in a format (podcasts) that are not particularly common in the world of cybersecurity. Hegel describes changes in tooling and tactics overtime and provides insight into the why questions behind these trends. The DoD needs to take advantage of these open source reports to better understand the cyber threat landscape we live in. The complete report discussed in the podcast can be found at the 401TRG website: <https://401trg.com/burning-umbrella/>. Another topic that is related to nation state hacking, intelligence, and cybercrime is “moonlighting.” This refers to nation state cyber actors using their skills and often times government systems to make money through cybercrime after “regular business hours.” This reality is mentioned briefly in a question and answer session during the 2nd Annual Billington International Cybersecurity Summit on March 30, 2017 in Washington, DC. The transcript of the discussion can be found here which points to China as the primary location for moonlighting cybercriminals.

CTC #16

Major General Charles J Dunlap Jr. wrote about his reflections on law and ethics in cyber war in the Air & Space Power Journal in 2013. In his article he makes the point that moral courage is rare, and yet cyber warriors need to exhibit this quality even more than physical bravery usually found in the military. He writes, “the law can provide an architecture, but only when honor and moral courage intersect can we truly rest assured that ethical principles worth defending are actually preserved.” This truth puts a lot of pressure on cyber operators to know not only what is in the law and how it applies to cyber (this is hard enough), but also to know what is moral and ethical in areas that are not defined in law or are ambiguous. Cyber operators, then, need to be concerned with how to developed sound ethical principles within themselves and instill those principles in others. This is where the article above, by Lt Col James Bottomlee, speaks into the cyber context. While nothing in the thesis speaks directly to the cyber domain, there are massive implications for cyber operators and the operations they perform. Bottomlee’s research of successful companies provides a rich pool to draw critical insights for the military. Until recently, the military was able to rely on families and culture to produce moral character in their new recruits that could then be applied to the military operations. But increasingly, the moral leaders in the military will need to be born and developed in the military. The Air Force and other military branches need to implement the key characteristics outlined in this thesis to “empower moral courage” such as defining core values, inspiring purpose, character-based mentoring, and wise culture management.