Chapter 5
A Geo-Political Analysis

ABSTRACT

Chapter 5 examines issues currently being encountered in the Middle East that demonstrate a cross-over between electronic warfare and cyber-warfare activities, affecting not only typical targets over the internet but also ships, aircraft, and unmanned aerial vehicles during the second decade of the new millennium. This overview provides examples of how cyber-warfare techniques are now being used in the battle space domain to affect geo-political situations within regions. The evidence shows how the cyber domain can influence real-life situations, taking its capabilities progressively just that one step further to hacker and state-sponsored cyber-attacks already witnessed against ICS cyber-physical assets. The viewpoint here draws upon historical stimuli and escalating political tensions now being encountered by opposing nations that could have a wider reaching impact.

INTRODUCTION

Over the past seven years, there have been escalating tensions in the Middle East especially since the United States pulled out of the nuclear deal with Iran (Whittaker, 2018). This action resulted in speculation over Iranian cyber-borne reprisals but left Russia, China, the United Kingdom, France, and Germany still committed to the original 2015 agreement (Efimchik, 2019). The main belligerent in the region is Iran, who has recently been disrupting global shipping lanes in the vicinity of the Strait of Hormuz. As a regional antagonist and littoral nation, the Iranians would seek to use the UN

DOI: 10.4018/978-1-7998-3979-8.ch005

Convention on Law of the Sea as a pretext to board merchant ships. This area can be up to 24 miles from their coastline instead of the traditional 12-mile limit (Dyer, 2019). In addition, the Iranian Republican Guard Corps (IRGC) based on Abu Musa island are suspected of using Electronic Warfare (EW) measures to jam and spoof Global Positioning System (GPS) Position, and Navigation and Tracking (PNT) data being received by tankers. This coerces merchantmen to deviate from their actual course into Iranian territorial waters (Crowe, 2019).

In the summer of 2019, Unmanned Aerial Vehicles (UAV) conducted strikes and alleged cruise missiles (Law, 2019a) attacks against the Saudi Arabian Aramco company's Abqaiq oil facility and Khurais oil field. The resultant shutdown of these facilities interrupted five percent of the world's oil supply (McKay & Tomlinson, 2019). Iranian-backed Houthi rebels in Yemen claimed responsibility as retaliation against the Saudi Arabian intervention in their civil war (CBS News & Associated Press, 2019; Cunningham & Noack, 2019). However, from a U.S. perspective, the *New York Times* provides a compelling case (Hubbard, Karasz & Reed, 2019) showing that there appears to be no evidence of the attacks originating from Yemen (Valero & Hamid, 2019). Analysis of delta-wing UAV debris indicates that the origins of this aerial asset was Iran (Turak, 2019), and the Iranians had actively been training their allies in the use of UAVs in the region (Hubbard et al., 2019). Therefore, the inferred finger of blame has been firmly wagging in Iran's direction, and this is not surprising since the Iranians have been early adopters of UAV technology over many years. Iran has even purportedly been using front companies to acquire foreign aero engines for their unmanned aircraft. As a result, the Iranians have many variants of UAV, including the Shahed 129 type that the United States has spotted participating in the conflict in Syria (Michel, 2013; Rawnsley, 2014).

There is also evidence of the Iranians using UAVs to undertake reconnaissance against U.S. naval warships in the Persian Gulf (CBS News & Associated Press, 2019b). This brings a new threat to U.S. forces because UAVs and drones have progressed from reconnaissance and intelligence purposes into dual homed weapons delivery platforms (Allen, 2013). This is certainly the case with regards to the US RQ-170 that the Iranians acquired and reverse engineered in 2011. Thereafter, the IRGC aerospace division copied and converted it for an unmanned combatant role to drop precision-guided bombs (Cenciotti, 2016). The European Council has already stated