Strategic Prioritization for the Naval Information Warfare Community
The Israeli Model (2,453 words)

The US National Security Strategy, National Defense Strategy and National Intelligence Strategy make it clear: emerging and disruptive technologies in the information domain are drastically altering the strategic environment. The CNO ensured alignment to these priorities in the establishment of The Design for Maintaining Maritime Superiority 2.0. The Naval Information Warfare Community's (IWC) role in achieving high velocity outcomes is narrowly scoped in the grand scheme but nevertheless, essential in keeping policymakers forward leaning in deciding the proper use of our military in foreign policy, and driving operators to find fix track and target potential adversaries. When I contemplated what the future of the Naval IWC should look like, simple observations and an exchange of ideas during a study abroad trip proved paramount.

Seven time zones away as the sun rises on the White House, Israel's intelligence leg of its Defense Force is hard at work. While Israel purposefully lacks a public National Security Strategy, its intelligence apparatus is very much in alignment with the State's priorities. Israeli intelligence has achieved a reputation as one of the world's preeminent organizations in the world through robust talent management systems and seamless public and private coordination. The IWC should follow suit.

In the months leading-up to my Cyber Power and National Security course in Israel mid June of 2019, worries of a State Department travel advisory clouded my excitement as the Strategic Environment became increasingly tense. For the red white and blue, the US's designation of the IRGC as a terrorist organization preceded the downing of a US drone over the Strait of Hormuz, increased military force posture in the CENTCOM AOR, and the reemergence of the tanker wars part II. [1] [2] [3] [4] For the Jewish Star, its designated spot in the "middle seat of an airplane" promulgated its perceived existential threats as the probability for conflict with the

---

[1] Cooper, Helene. "What We Know About Iran Shooting Down a U.S. Drone." The New York Times. June 20, 2019. Accessed July 2019. https://www.nytimes.com/2019/06/20/us/politics/drone-shot-down-iran-us.html.

[2] "Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization." The White House. Accessed July 2019. https://www.whitehouse.gov/briefings-statements/statement-president-designation-islamic-revolutionary-guard-corps-foreign-terrorist-organization/.

[3] "Statement From Acting Secretary of Defense Patrick Shanahan on Additio." U.S. Central Command. June 18, 2019. Accessed July 2019. https://www.centcom.mil/MEDIA/STATEMENTS/Statements-View/Article/1879460/statement-from-acting-secretary-of-defense-patrick-shanahan-on-additional-force/.

[4] O'Grady, Siobhán. "The U.S.-Iran Showdown: What's Happened in the Week since Two Tankers Were Attacked." The Washington Post. June 21, 2019. Accessed July 2019. https://www.washingtonpost.com/world/2019/06/18/us-iran-showdown-what-happened-after-two-tankers-exploded/?utm_term=.a194d5c1ba90.

IRGC's covert extension (Hezbollah) increased in parallel with that of the US and Iran. Furthermore, the Palestinian Authority boycotted the simultaneous US led Middle East economic workshop in Bahrain, consequently raising the probability for conflict in disputed settlements in the West Bank and between IDF and Hamas in the Gaza Strip. [5]

Two incidents in particular could not have occurred at a better time and provided enriched conversations between academics and practitioners alike in one of the cyber capitals of the world, Tel Aviv. The first instance was one month prior to arrival in Tel Aviv for Cyber Week and was centered around a tweet from the IDF stating "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where Hamas cyber operatives work. HamasCyberHQ.exe has been removed." This particular public response by the IDF marked a notable change in cyberwarfare as we know it- a physical kinetic strike in response to a non-kinetic attack in the cyber domain. [6] Furthermore, the United States choose to respond to the shootdown of a four-million-dollar drone with a cyber attack targeting Iranian Intelligence computer systems. [7] Academics, policy makers, and warfighters have been raising the questions regarding proportionality, rules of engagement, and deterrence in the cyber domain for decades and these two actions action could unknowingly be writing unofficial normative response mechanisms and calibrating where the threshold of war resides. Two things are clear: cyberwarfare is fully integrated across the full spectrum of conflicts (i.e. state, non-state, proxy state) and that information warfare is at the tip of the spear. However, it is important to note that the cyberwarfare is not information warfare and that information warfare is a facilitator for cyberwarfare. While much of my references revolve cyberwarfare in the context of Israel, the same concepts can be applied to information warfare.

The purpose of my travels to the Holy Land was to be a participant in Cyberweek 2019 at Tel Aviv University, the 9th international conference aimed to pioneer strategies and solutions to risks and opportunities created in the cyber domain. Upon entrance into the main plenary, I observed three individuals near one of Israel's "Start-Up" company booths after having just ordered a fresh cup of espresso. The three individuals were the current Director of Israel's National Cyber Directorate, Head of the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University, and the CEO of Team8, a renowned Israeli cybersecurity Start-up. The common thread between the three gentlemen was prior service in Unit

---

[5] Moore, Jack. "Bahrain Readies to Host Trump's Much-maligned Bid for Middle East Peace." The National. June 25, 2019. Accessed July 2019. https://www.thenational.ae/world/mena/bahrain-readies-to-host-trump-s-much-maligned-bid-for-middle-east-peace-1.878441.

[6] Doffman, Zak. "Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First." Forbes. May 06, 2019. Accessed July 2019. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#16f1731aafb5.

[7] Barnes, Julian E., and Thomas Gibbons-neff. "U.S. Carried Out Cyberattacks on Iran." The New York Times. June 22, 2019. Accessed July 2019. https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.

8200, Israel's Cyber/Signals Intelligence division. Later on, in the morning, the Head of ICRC presented the Award for Achievement in Cyberspace to the Director of the Mossad, followed by remarks by Prime Minister Netanyahu, highlighting Israel's prominence in cyberspace. What struck me was the apparent cohesion and unity between the public, private, and academic sectors that have arguably been the underpinnings for Israel's rise to economic prosperity and military dominance in the region.

The path to prominence in Israel begins with the hopes and dreams of young children to join these prestigious organizations. As early as age 14, IDF Intelligence Organizations begin testing and evaluation for highly sought-after positions during obligated conscripted service. Talent identification and recruitment methods from organizations such as 8200 and the Mossad ensure that the right people are placed in the right positions. I had the privilege of hearing testimonies from former 8200 members that emphasized – "there is nothing like the training and investment the state dedicates in developing unique skill sets for the future members of one of the world's leading intelligence organizations". Furthermore, regardless of career commitment in IDF's intelligence services, talent retention exists in that many members serve their mandated time and become entrepreneurs to fuel the Start-Up nation and Israel's economy. The large majority of companies focus on some aspect of emerging technology or cybersecurity. These testimonies explain that personal success feeds collective success to the State of Israel, which is all derived from the responsibility placed in 18-20 year old hands and their freedom to maneuver/innovate during times of conflict- much of which could result in life or death of their counterparts, let alone the mere existence of the state of Israel. When National Security Issues arise, the solution may end up sourcing from a private cybersecurity firm in the detection, attribution, or response of non-kinetic fires. The dialogue between 8200 and X, Y, or Z private cyber firm will often initiate with a warm greeting of two individuals who used to sit side-by-side in the depths of the IDF's Intelligence apparatus which will subsequently be followed by actionable offensive, defensive, or exploitation intelligence operations. Furthermore, the IDF's testing of new tools, tactics, techniques, and procedures may often times be conducted by the Start-up emerging tech firm, or vice versa as a proof of concept for the entrepreneur at the Start-up before marketing the product/service for business.

My encounters with profound intelligence professionals began in Switzerland during my layover, preceding my arrival in country as a border control agent mapped every wrinkle in my skin, immediately determined my heart/breathing rate without a stethoscope, and determined the contents of my last meal based on the smell of my breath during a security questioning and inspection before boarding the plane. It continued during a marketing pitch of a Cyberbit employee, started by a former Director of Mossad, which provides an infiltration and mapping service that portrays TTP's of how an adversary will reach the "crown jewels" of your network. Notably, it ended with a resonating quote from a former member of Israel's National Security Council during the Obama administration

during a guest lecture regarding US influence in the Middle East: “The United States has a lot of clout”.

To retain that clout, the IWC can develop similar models of talent recruitment and development, and cohesion with the private sector to receive the same national prestige that 8200 and Mossad do in Israel. However, the model will look different due to voluntary service and an unscalable demographic comparison between Israel and the US. Nonetheless, this can still be achieved and should be the IWC’s priority in the current strategic environment to align with the CNO’s Maritime Superiority 2.0. The IWC should embark on a two-pronged strategy: one at recruiting, acquiring, developing, and retaining talent and the other to enhance its relationship with the private and academic sector. The focus on talent in the IWC apparatus most evidently “Strengthens our navy team for the future” which transcends itself into “strengthening naval power at and from the sea”. The focus on building partnerships with private and academic equities “expands and strengthens our network of partners” which catalyzes an integrative force for “achieving high velocity outcomes”. Regardless of if you are supporting policy development in the nation’s capital, naval strategy at a Combatant Command, naval operations at sea, or acquisition of the next generation collection suite, the caliber of people involved in the process and the relationships between them are the most critical factors yielding high success rates.

First and foremost, selection into the IWC will need to be competitively precise. Competitively precise means that the IWC becomes an unrestricted line community. Competitively precise means that selection into the community no longer occurs as a result of a lack of medical readiness. Competitively precise means that the IWC is no longer an option for the redesignation pocer board process. The notion of the term “restricted” implicitly conveys to services members a genetic potential limitation associated with the prescribed community. Information warrior’s innovation and freedom to maneuver in the electromagnetic spectrum and cyberspace are requirements in current strategic environment; one in which conflict will persistently exist below the threshold of war in the “gray zone”, where non-kinetic battles will ensue against adversary nation state information warriors. Furthermore, passive submission to questionable candidates’ entry into the community degrades our prestige. Even with such a small community, mishaps slide through the cracks as a result of subpar human resource mechanisms and degrades the IWC’s reputation. The IWC needs to embark on an active pursuit of talent, ensuring the right people with the right skills are identified at an early age and recruited. A 21st century strategic messaging approach to convey the old public affairs propaganda of “join or die” will be prudent in identifying young talent and instilling purpose in their lives. Outreach programs should span middle school through graduate school across the nation with screening mechanisms in place that consider skill sets such as physical fitness, STEM proficiencies, critical thinking ability, and emotional intelligence in order to acquire top notch talent and place them in appropriate career tracks. Specialization over generalization should be prioritized across IWC officer designators based on identified strengths in

prospective candidates BEFORE entrance into the navy. Specialty career tracks in cyber, space, electromagnetic maneuver warfare, C4ISR-T, and 1-3 intelligence disciplines (i.e. GEOINT and MASINT or OSINT, SIGINT, HUMINT etc) should be initiated. This is not to discount the value of generalization, the current trend in development of naval officers, because generalization should be a specialization within itself. The specialized generalists should serve as the connective tissue across the INT disciplines, subset speciation across information warfare, other missions the navy and partner service branches are tasked with, and the Intelligence community writ large as to prohibit stove piping.

To expand and strengthen our network of partners, the IWC should open additional opportunities associated with the Secretary of the Navy's Tours with Industry. The active duty tours will be specific to the IWC and expose officers to private company cybersecurity/intelligence firms to include but not limited to FireEye, Symantec, Boeing, Bank of America, Google, Facebook, and Booz Allen Hamilton. The law of increasing returns to scale applies from all perspectives by enhancing corporate-government relationships and increasing the exchange of ideas and technology. The future relationships between private and public sectors will be pivotal because of the indistinguishable Rule of Engagement that the adversary uses in times of peace and times of war. The adversary views the information space as a vector of attack against civilian infrastructures that may be linked to the navy directly or indirectly. The first time that a Naval IWC professional is required to work side by side with the private sector should not be directly after a debilitating attack. In parallel, specialty liaison billets should be created to help integrate efforts between private sector and navy IWC professional. This builds from the already established SECNAV private sector tour initiative but emphasizes development in high tech skills that will be called upon in non-kinetic fires. For example, an IWC officer serves a tour at one of the aforementioned companies, working with cutting edge tools and processes in order to prepare for emerging technological challenges presented in the strategic environment. Following this tour, the officer will develop the requisite skills to lead the initiative in establishing cohesive, rapport building public-private networks that encompass our industry partners in an information secure environment.

Simultaneous to private sector tour, additional lifelines can be created by investing in relationships with already existing Veteran's networks at private companies and industry partners. This can be done simply by including them in networking events in DC, San Diego, and Norfolk. Additionally, inclusive Naval IWC quarter/bi-annual/annual conferences would cultivate stronger connections with researchers from leading academic institutions and developers from industry giants with the long-term goal of establishing academic research labs specific to naval IWC research. An interdisciplinary approach should be taken, since competitive advantage in the information environment comes from fully understanding the intersection of politics, intelligence, law, engineering, computer science, and psychological factors that influence manipulation of the information domain. Opening the aperture of participants encourages the exchange of knowledge and

ideas that proves invaluable over time and cannot be overlooked when attempting to strategically orient the IWC's priorities.

The naval IWC absolutely needs to recognize that that talent management and integrative public-private sector integration are prerequisites in seizing the information environment of the future. Next year, I hope NAVPERS not only sends a few representatives to all the naval IWC commands, but also embarks on a talent scavenger hunt to job fairs and schools in search for the next generation of information warriors. Next year, I hope my colleagues have the opportunity to be selecting for a Naval IWC Private Sector Industry tour at FireEye. Next year, I hope to see the Commanding Officer of the Information Warfare Development Command, Commanding Officer of Fleet Cyber Command, Director for MIT's Research Centers, and CEO of Symantec and Booze Allen all sharing a cup of coffee and discussing the threats of today and challenges of tomorrow, just like at Cyber Week 2019 in Tel Aviv. This US tailored, Israeli-based two-pronged strategy is not all encompassing and intended to provoke larger discussions of leaders in how to strategically focus the community in alignment with the CNO's lines of effort.