The Challenge of the Indigenous Arms Industry: The Ascendant and Dependent Classes

David Davidian
March 23, 2017

Just as Niccolo Machiavelli noted the unreliability of mercenaries [1] and interpretations of Sun Tzu [2] claiming a mercenary's real value is not more than half a native soldier, one can extrapolate from these observations to deduce that the most effective arms industry is indigenous. While this may not be much of a revaluation, its implementation, especially in developing countries (and even developed countries), is becoming exponentially difficult. The gap between the necessity for manufacturing indigenous arms and the ability to deliver them is widening and has been since the end of WWII. This gap is not between first- and third-world states. To be more precise, if one looks at the history of weapons development since the end of WWII, one sees that countries that have had uninterrupted arms development are those that have been able to build upon and maintain military research and development programs and can deliver continuously advanced weaponry to the field. It is nearly impossible for a newly established state or an established state that wishes to enhance its defensive capabilities with serious indigenous development to do so at the same rate as established state industries, for the ever-increasing rate of change in technology is fostered by “ascendant-class states”. An exception to this may be Israel, but this is due to its extensive ties with the US military industrial complex. The widening of the technology barrier is in the interest of ascendant-class states such as the US, Russia, and China as they are the leading arms exporters to the “dependent-class states”.

Where has this left the dependent-class states, specifically those that have budgets, technology, development and management capabilities, and inevitably the political necessity for weapons? Given a fortuitous combination of items from the preceding list the best bang-for-the-buck is to develop nuclear weapons. Israel's nuclear program [3] began as far back as the 1950s, accelerating after the 1967 Six Day War. Some states move from dependent-class to the nuclear club sometimes at the expense of feeding their own people. North Korea is an example. If Iran were not effective in its indigenous weapons program and uranium enrichment capabilities, it might be relegated a Middle East backwater subject to a Persian Spring.

We have seen this spelled out clearly with India and Pakistan. Both have nuclear weapons. India claims to have hydrogen bombs [4] of varying yields, yet it must import its best fighter jets as does Pakistan. While joint development or licensing of technology seems a reasonable compromise in some scenarios, ascendant-class states limit the amount of technology that is exposed. Many examples can be cited, but earlier this month joint development of an Indian-Russian fifth generation fighter jet stalled over Russian concerns that its stealth technology would be compromised. [5] Pakistan was hoping it would acquire the capability to build a state-of-the-art fighter jet from scratch in their joint JF-17 Thunder program with China. This didn't happen. “...PAF [Pakistani Air Force] understood that it cannot build a backbone fighter via imports.” [6] A licensing agreement between Azerbaijan's Defense Ministry and Aeronautics Defense Systems of Israel for the local assembly of Aerostar and Orbiter UAVs (Unmanned Aerial Vehicles) in Baku still has 70% of the components produced in Israel. [7]

These are strong reminders of what Machiavelli and Sun Tzu observed hundreds and thousands of years ago, respectively. The dependence resulting from not reinventing one's own wheel can be a gating factor as the ascendant-class can modulate the game.

What of those states that have limited resources, and/or never had or lost their research and production capabilities to sustain a limited indigenous arms industry? These states would rank below dependent-class status. In some cases, it makes little sense in both time and effort to match technology-for-technology with a state's perceived enemies. For example, if state A has advanced tanks or other heavy weaponry, rather than to match or exceed it in quantity and/or quality, state B could use ultra-sensitive vibration and triangulation processing to locate tanks in motion from many kilometers away and target them with standard artillery. When the enemy's advanced tank is disabled and captured, further inspection and investigation could provide methods for more effective destruction. Most offensive military UAVs have anti-radiation protection. However, a UAV must either be directed or self-identify a target. Considering that the methods available for targeting are based on technologies associated with radar, ladar, electro-optical sensors, GPS, etc., rather than to match the enemy’s advanced UAV systems, creating ways of disabling or degrading their tracking and target acquisition may be the way to go in defending against such technologies. Inexpensive, yet effective, (non-nuclear) directed EMP (Electro Magnetic Pulse) systems may be enough to temporarily degrade or at least cause directional errors large enough to divert the UAV. Wide field laser weapons [8] meant to blind soldiers (banned by the UN) could damage electro-optical sensors, adapted for use in combination with other defense mechanisms. Such techniques can be an alternative to developing a top of the line military UAV industry.

Then, there is cyber warfare. Some call this the great equalizer because cyber attacks are anonymous, effective, deniable, and entire state infrastructures can be taken down with a keyboard. The United States, China, Russia, and Israel are on cyber warfare technology's leading edge. Some of this is very overt. Job postings for several years in the United States include a new position called an “ethical hacker”. Targeted cyber weapon efforts such as Stuxnet [9] require the prowess of a sizable state. This is due to the combination of wide systems expertise, cyber hacking technology, and human intelligence required to stage such a debilitating weapon. Less challenging, yet devastating, attacks can be the work of a single cyber soldier. Cyber warfare attacks have been reported on infrastructures in Syria, Ukraine, Estonia, Burma, Iran, Japan, Israel, South Korea, US, Georgia, etc. If there is such a thing as collateral damage from cyber attacks, the following story should shed light on this. While I was on a visit to the Republic of Georgia in 2008, hostilities between Russia and Georgia commenced. The Russians began the equivalent of a denial-of-service attack on the Georgian internet infrastructure. This resulted in the inability of Georgians to access facilities such as email; but, most importantly, accurate information simply wasn't available. One might as well have been in the dark ages, for local TV reverted to showing black-and-white movies of Georgians defeating the Persians hundreds of years earlier. Russian cable channels were severed. Rumors became “reality”: flour imports were rumored halted, which caused a run on bakeries at 2pm one morning; word on the street was the country was low on beans, and within hours the price of beans in Tbilisi stores became astronomically high; Russian fighter jets were launched from air bases in Armenia (this was specifically announced as false on Georgian TV). If collateral cyber damage from not having internet access to at least neutral information were actually planned, it

alone could cause erroneous decisions to be made based on false or incomplete information.

Georgia did not need a classical army of soldiers, weapons and tanks to mitigate this denial-of-service attack. I am sure lessons learned will be implemented as the boundary between ascendant-class and dependent-class or below is not easily defined in cyber warfare.

Finally, there are non-state actors. Non-state actors are either given weaponry or must secure them financially. As proxies for regional or international powers, non-state actors are subject to the vagaries of their patrons. However, as the line between state-of-the-art state-sponsored hackers and those of an astute individual is blurred, the capability of non-state actors to create infrastructure chaos is real. Six months ago, Syrian hackers claimed responsibility for hacking into Belgian news sites. Only last month, it was reported that ISIS-affiliated hackers attacked various governmental sites in the UK. [10] It could take only a few more keystrokes to hack into UK's power distribution grid even though it is actively protected against such attacks. Military and defense secrets are the most fleeting of all.

The world is increasingly technologically complex. It would be remiss of established states not to maximize their indigenous defense capabilities – if – such states are determined to minimize their dependence on the ascendant-class. Minimum dependence enhances the ability to defend one's own interests.

David Davidian is an Adjunct Lecturer at the American University of Armenia. He has spent over a decade in technical intelligence analysis at major high technology firms

[1] The Prince, page 20
[2] Art of War; 9. The Army on the March
[3] Israel's Worst-Kept Secret
[4] Nuclear Anxiety: The Overview; India Detonated a Hydrogen Bomb, Experts Confirm
[5] Full tech transfer could derail Indo-Russian fifth-gen fighter program
[6] What did Pakistan gain from the JF-17?
[7] Azeris get Israel UAVs built under license
[8] How the US Quietly Field Tests 'Blinding' Laser Weapons
[9] An Unprecedented Look at Stuxnet, the World’s First Digital Weapon
[10] Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images