National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE RUSSIAN HYBRID MODEL AS A TOOL FOR REGIONAL POWERS

LCdr Gareth Jarvis

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE RUSSIAN HYBRID MODEL AS A TOOL FOR REGIONAL POWERS

LCdr Gareth Jarvis

Word Count: 3298

Compte de mots: 3298

THE RUSSIAN HYBRID MODEL AS A TOOL FOR REGIONAL POWERS

Introduction

Russia's ongoing effort to regain influence within the traditional Soviet sphere via *Russian New Generational Warfare* (its interpretation of hybrid warfare)[1] demonstrates that states can advance their interests despite conventional military weakness. The success of the Russian Ukrainian campaign and its coordinated use of irregular warfare, limited campaign objectives, the cyber domain and key defensive military capabilities provides a viable and achievable model for medium powers looking to expand their regional influence.

Iran is one such power. This paper will apply the *Russian New Generation Warfare* model to Iran. It will outline the similarities between Russia and Iran's relative capabilities, and how the Russian model provides Iran a viable hybrid warfare blueprint that it can follow to increase its standing as the regional power within the Middle East. As hybrid warfare consists of many different capabilities, this paper will focus on three key capabilities that Russia leveraged and which Iran is capable of integrating into its campaigns; cyber-warfare, irregular warfare and Anti-Access/Area Denial (A2/AD) capabilities.

Russian New Generation Warfare: Background and Motivator

The end of the cold war and the collapse of the Soviet order hollowed out Russia's military capabilities and global influence. The drastic cutbacks, elimination of 400 000 officer

[1] Sometimes referred to by Russians as *non-linear warfare*.

positions,[2] equipment obsolescence, and rampant desertion degraded the effectiveness of the military and destroyed its expeditionary capabilities. This coincided with a reduction of Russian influence on the world stage and within its traditional Eastern European sphere of influence.[3] Rebuilding this influence and containing the involvement of other states within its historical sphere of influence became a significant Russian motivator.

Russia's campaigns in *Chechnya* (1994-1996 and 1999-2000) highlighted the weaknesses of the Russian military. The performance of conscript soldiers was poor and the Russian forces were challenged in achieving their objectives.[4] These difficulties persisted during the *South Ossetian War* (2008). Military reforms were launched in 2009[5] however the pace was slower than anticipated due to poor economic conditions.[6]

Russia has adopted its form of hybrid warfare to allow for limited campaigns using irregular warfare (to apply military pressure) and the cyber domain (both offensively and to generate social pressure)[7] while using A2/AD weapons to prevent direct response and to restrict the ability of other states to become involved.

Russian Military Technology and Anti-Access/Area Denial Systems

Russia continues to build advanced weapon systems such as the Sukhoi Su-27/Su-35 but the adoption of modern systems by the Russia military has been slow. One group of weapons

---

[2] Marcel de Hass, *Russia's Military Reforms: Victory after Twenty Years of Failure,* (The Hague: Institute of International Relations, 2011), 8

[3] Stephen F. Larrabee, "Russia, Ukraine, and Central Europe: The Return of Geopolitics," last modified 15 April 2010, https://jia.sipa.columbia.edu/russia-ukraine-and-central-europe-return-geopolitics.

[4] Olga Oliker, *Russia's Chechen Wars 1994-2000, (*Santa Monica, CA: RAND Corporation, 2001), 43-45.

[5] Jonas Grätz, "Russia's Military Reform: Progress and Hurdles." *CSS Analyses in Security Policy*, no. 152 (April 2014): 1-2

[6] Ibid., 3-4.

[7] US Army Asymmetric Warfare Group, *Russian New Generation Warfare Handbook* (Fort Meade, MD: Department of Defence, 2016), 4.

that Russia has continued to adopt are A2/AD systems. This includes modern versions of the S-300 and S-400 theatre level long range anti-air platforms capable of engaging aircraft, cruise missiles, and ballistic missiles out to hundreds of kilometres, Iskander-M ballistic missiles and SS-N-26/ Bastion-P anti-ship cruise missiles. To leverage this capability Russia has established A2/AD complexes in Kaliningrad and the Crimea.[8] Kaliningrad denies access to the eastern Baltic and threatens NATO's access to Eastern European *aerial ports of disembarkation* (APODs) and *sea ports of disembarkation* (SPODs) pushing NATO's abilities to rapidly deploy troops as far back as the western Polish border[9] and dramatically increasing the time required to respond to situations in the Baltic states, the Ukraine, or Poland. The Crimean A2/AD complex restricts access to the western Black Sea and isolates the southern Ukraine.[10]

Russian Cyber Capabilities

Russia has developed extensive cyber including significant abilities in the sub-domains, *cyber-espionage*, *cyber-disruption/cyber-attack* and *social and political effects* (via social media, media, and other channels). Russia's current capabilities are rated as advanced with the potential to cause an opponent catastrophic impact.[11]

Russia's first sustained demonstration of its cyber capabilities occurred during the 2008 conflict with Georgia. Russia's offensive cyber-attacks were generally successful but its overall information warfare capabilities were lacking and it lost the social media conflict.[12] Russian

[8] Ian Williams, "The Russia – NATO A2AD Environment," Center for Strategic and International Studies Missile Threat, Last modified 3January 2017, https://missilethreat.csis.org/russia-nato-a2ad-environment.

[9] Ibid.

[10] Ibid.

[11] Jon Condra, *Business Risk Intelligence Decision Report 2017 End Of Year Update*, Flashpoint, 2017, 8.

[12] Julien Nocetti, *Guerre de l'information : le Web Russe* (Paris/Brussels: Centre des études de sécurité and Conseil Supérieur de la Formation et de la Recherche Stratégiques, 2015), 25-27.

capabilities in the Ukrainian conflict have been more complete targeting voting systems, industrial control systems (power plants), and media and commerce (via denial of service attacks).[13] An extensive *social and political effects* campaign was conducted via social media and by restricting Ukraine access to the internet and broadcast media.[14]

Russian Sponsored Irregular Warfare

Russia uses irregular warfare to apply military pressure, destabilize opponents and to build influence. The Ukrainian campaign offers several examples. Unidentified (although attributed to Russia) "polite green men" seized key political, economic, and military locations in the Crimea just prior to the Crimean governments request for Russian assistance.[15] Once the Crimea was secured and the campaign moved to Eastern Ukraine, Russian funded mercenaries and Russian-aligned militias supported by deniable special forces advisors[16] were used to support the "Ethnic Russian" insurgency.[17]

Iran: Background, Historical Capabilities and Motivators

Under the Shah, Iran was well on the way to becoming a US supported regional superpower. The Iranian military was (relatively) well trained and well equipped with US and European equipment. The 1979 Revolution lost Iran the support of its Western armourers and the

[13] Marie Baezner and Patrice Robin. *Cyber and Information warfare in the Ukrainian conflict (*Zurich: Center for Security Studies, 2017), 7,13-14.

[14] Many significant Ukrainian communication links connected to the broader global network via Russia. Baezner and Robin. *Cyber and Information warfare in the Ukrainian conflict…,* 16.

[15] Hall Gardner, "Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict." *Research Paper 123*, NATO Defense College (December 2015): 10.

[16] Although Russia eventually deployed some heavy formations to the Ukraine.

[17] Ibid., 10-11.

officer purges directed by the *Ideological-Political Directorate of the Armed Forces* (establish by the clerics to establish control over the military)[18] rapidly eroded the effectiveness of the Iranian forces.[19] The establishment of the *Islamic Revolutionary Guard Corps* (IRGC) as a lightly equipped parallel force tasked with defending and exporting the Iranian Revolution provided the Iranian government with an alternative military force and further reduced the influence of the Iranian military. The nine year Iran-Iraq war consumed equipment and supplies that could not be replaced from Western sources due to sanctions. By 1988 the military and the IRGC were poorly equipped but experienced. [20] A five-year $10B rearmament program announced in 1989 faltered due to Iran's continued economic problems however Iran was able to acquire significant, if primitive, A2/AD weapons in the form of Chinese CSS-8 short ranged ballistic missiles and HY-2 Anti-Ship Missiles.[21]

Historically Iran has viewed itself as a regional power with a large sphere of influence within the Middle East. Iran resents the growth of Saudi regional influence over the last twenty five years and views itself as the prime guardian of true Islam and Shia populations. Western intervention in the Middle East (including support of Sunni regimes) and especially the US's intervention and regime change in Iraq is seen as a direct threat to Iran and its interests.[22]

---

[18] Plus wide scale defection and self-exile of senior officers.

[19] Hashim, Ahmed S. "The Iranian Military in Politics, Revolution and War, Part Two." Middle East Policy Council XIX, no. 3 (Fall 2012): Last Accessed 20 May 2018, http://www.mepc.org/iranian-military-politics-revolution-and-war-part-two.

[20] Ibid.

[21] Michael Eisenstadt, *Iranian Military Power: Capabilities and Intentions* (Washington, DC: The Washington Institute for Near East Policy, 1996), 1, 29.

[22] Ibid., 3-4.

Iranian Anti-Access and Area Denial: Leveraging the Choke Point

Iran's geography consisting of the entire eastern side of the Persian Gulf (Gulf) coupled with the 300nm natural choke point of the Strait of Hormuz (Strait) has allowed Iran to deploy anti-access weapons to restrict access into and out of the Gulf. The 1980's *Tanker War* and *Iran-Iraq War* saw Iran use a combination of sea mines laid by improvised mine layers of the *Islamic Revolutionary Guard Corps Navy*, sea skimming anti-ship missiles and swarm speedboat attacks on shipping within the Gulf and Strait.[23] The mining of *USS Samuel B Roberts (*a USN frigate) and damage to multiple oil tankers demonstrated Iran's ability to cheaply and covertly block the Strait at least temporarily.[24]

Iran continues to develop A2/AD capabilities to solidify its ability to restrict access to the Gulf. Its original semi-obsolescent Silkworm missiles have been supplemented by more modern Iranian built missiles derived from Chinese designs. [25] It looks to supplement this by acquiring advanced sea mines, armed drones (both aerial and small boat), submarines, and torpedoes.[26] Iran also seeks to acquire and natively develop advanced theatre level anti-air missile systems. Recent acquisitions such as Russian S-300 based systems can reach far into the Gulf, Gulf of Oman, and Iraq and can restrict access to the airspace of the Gulf States. Iran continues to develop ballistic missiles (both conventional and anti-ship)[27] with the ability to strike targets such as assembly points and APODs/SPODs throughout the region. Iran has supplied ballistic

---

[23] Ronald O'Rourke, "The Tanker War." *Proceedings Magazine*, May 1988, Last Accessed 10 May 2018, https://www.usni.org/magazines/proceedings/1988-05/tanker-war.

[24] Bradley Peniston, "The Day Frigate Samuel B. Roberts Was Mined", *USNI News*, Last updated 22 May 2015, https://news.usni.org/2015/05/22/the-day-frigate-samuel-b-roberts-was-mined.

[25] Office of Naval Intelligence, *Iranian Naval Forces: A Tale of Two Navies* (Washington, DC: Department of Defence, 2017), 32.

[26] Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Washington: U.S. Government Printing Office, 2018), 19.

[27] Zachary Keck, "Meet Iran's "Carrier Killer": The Khalij Fars," Last modified 11 May 2013, https://thediplomat.com/2013/05/meet-irans-carrier-killer-the-khalij-fars,and Missile Defense Advocacy Alliance, "Fateh-313", Last modified 3 March 2017, http://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/iran/fateh-313.

missiles (as opposed to rockets)[28] and anti-ship missiles to proxies such as Hezbollah which launched a 2006 attack (with technical support from the IRGC) on an Israeli ship off the coast of Lebanon.[29]

Iranian Irregular Warfare: Decades of Proxies

Iran has a history of using irregular warfare and proxies to support Iran's interests in the host country and to act as a deterrent against foreign involvement. The IRGC, via its Quds special forces branch, has been an active participant in proxy conflicts, notably Lebanon[30] both to advance Iran's interests and to counter both Syrian and Israeli influence.[31] This support has evolved from arming and training proxies to IRGC officers serving as command elements for local forces as recently demonstrated within Syria.[32]

One notable Iranian success has been Shia militias within Iraq. The Badr Brigade established in the 1980s using Iraqi defectors and Iranian officers has evolved to be a significant power block within Iraq. The Iranian established and Shia dominated *Popular Mobilization Force* militia gained control of the Iraqi Interior Ministry and its subservient Federal Police Force.[33]

---

[28] Center for Strategic and International Studies, "Fateh-110," Last modified 8 September 2016, https://missilethreat.csis.org/missile/fateh-110.

[29] Mark Mazzetti and Thomas Shanker, "Arming of Hezbollah Reveals U.S. and Israeli Blind Spots," *New York Times*, 19 July 2006.

[30] Matthew McInnis, "The Strategic Foundations of Iran's Military Doctrine," in *Gulf Security after 2020*, (London: The International Institute for Strategic Studies, 2017), 5.

[31] Ibid., 7.

[32] Paul Bucala, "Iran's New Way of War in Syria," American Enterprise Institute and the Institute for the Study of War, 2017, Last Accessed 12 May 2018, http://www.understandingwar.org/sites/default/files/Iran%20New%20Way%20of%20War%20in%20Syria_FEB%202017.pdf, 5.

[33] Ranj Alaaldin,"How Will Iraq Contain Iran's Proxies?" *The Atlantic*, last modified 22 February 2018, https://www.theatlantic.com/international/archive/2018/02/the-man-who-could-help-rebuild-iraq/553799 and Tom O'Connor, "U.S. Soldiers Under Threat As Iran Allies Join Iraq Military With Plans To Kick Americans Out."

Iranian Cyber: Potent But Unfocused

Iran has long possessed cyber capabilities especially in the sub-domains of espionage and cyber-attack. Iran's capabilities are ranked technically sophisticated with the ability to cause significant damage.[34] Although Iran has undertaken some cyber provocations against Western nations it predominately uses its capabilities against regional rivals such as the 2016 and 2017 cyber-attacks that damaged government and private sector networks in Saudi Arabia.[35] Its operational model uses Iranian non-state actors under the control of the IRGC. The use of cyber is often opportunistic, attacking regional competitors due to perceived weakness rather than as part of a larger coordinated campaign.[36]

Iran cyber capabilities are less developed in the sub-domains of psychological warfare and social engineering operations. Most social media activities have targeted Iranians viewed as a risk to the regime such as internal dissidents, reformist politicians, outspoken members of the Iranian diaspora, or Iranian detractors overseas. Iranian social media operations are often focused on removing Iranian access to social media and identifying dissidents.[37]

Newsweek, Last modified 9 March 2018, http://www.newsweek.com/us-soldiers-under-threat-iran-allies-join-iraq-military-kick-americans-out-839255.

[34] Jon Condra, *Business Risk Intelligence Decision Report 2017…*, 6.

[35] Director of National Intelligence, Statement for the Record…, 6 and George Seffers, "Russia, Iran and North Korea Bolder in Cyber Realm." *Signal*, 13 February 2018, https://www.afcea.org/content/russia-iran-and-north-korea-bolder-cyber-realm.

[36] Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington: Carnegie Endowment for International Peace, 2018), 17, 32.

[37] Ibid., 42-48.

Similarities between Iran's Russia's Hybrid Warfare Capabilities

Both Russia and Iran have developed hybrid warfare capabilities to address similar conditions. Both have large militaries that struggle with obsolescence and quality, especially compared to western states. Both desire to establish (Iran) or re-establish (Russia) spheres of influence within regions that they historically view as theirs.[38] Both are using the asymmetrical nature of hybrid warfare to counter the perceived dominance of the larger powers within the region (the US and US aligned Gulf states in the case of Iran and NATO and NATO leaning Eastern European states in the case of Russia).

Although not as advanced or numerous as Russia's A2/AD weapons, Iran's deployment model is similar. Iran can temporarily restrict transit into and out of a maritime choke point, use its theatre level air defences to interdict the airspace of its Gulf neighbours and its ballistic missiles to threaten APODs, SPODs, and assembly areas for any force amassing to strike Iran. The Iranian military, especially the IRGC, have a long history of supporting irregular warfare and using proxy forces to advance Iran's interest. Iranian advisors are ubiquitous within failed or failing states within the region and Iran's promotion of Shia/Iranian aligned militias is comparable to Russia's use of ethnic Russian militias in Eastern Ukraine. Iran has developed its cyber capabilities to enable attacks on the infrastructure and commerce of its neighbours. Unlike Russia, Iran has not demonstrated the ability to combine its cyber capabilities into a coordinated campaign or that it can engineer sustained social impact via cyber operations.

Unlike Russia, the leadership of the various Iranian military and government agencies is fragmented with intense rivalry between the regular military and the IRGC. This was partially by

[38] Secretary of Defence. *Unclassified Report on the Military Power of Iran 2010*. (Washington: Department Of Defence, 2010), 1.

design due to Iranian fears of leadership decapitation attacks from the US.[39] The lack of a central coordinating command has caused Iran to use its capabilities in isolation rather than as part of a comprehensive campaign. Iran recognized this and in 2016 it started a process of reorganizing its command structure, general staff and unifying functions into specific commands.[40]

Potential Use Case: Gulf States

The Russian campaign in Crimea has demonstrated how a well targeted hybrid campaign can succeed.[41] One potential Iranian use case for an effective hybrid warfare campaign is disrupting the Saudi dominated *Gulf Cooperation Council* (*Council*) by isolating one of the *Council's* members and increasing Tehran's influence at the cost of Riyadh's. Iran cyber-capabilities could be used to engineer social unrest and fiction between the targeted state and other council members. Iran could offer to provide military assistance to the threatened state or could cause additional friction by supporting insurgency within one of the Gulf States. Iran could threaten to close the Strait using its A2/AD capabilities, placing economic pressure on *Council* states and isolating them from rapid US intervention while Iran's ballistic missile capabilities could threaten *Council* capitals or oil export facilities.

Elements of this use case have occurred over the last couple of years. The ongoing standoff between Qatar and other council members over claims that Qatar is too friendly with Iran demonstrates that the *Council* not a unified organization and external factors could shape its policies and membership. Cyber-attacks were one trigger of this crisis when fake news articles

[39] Paul Bucala and Marie Donovan. "A New Era for Iran's Military Leadership". Last modified 1 December 2016, https://www.criticalthreats.org/analysis/a-new-era-for-irans-military-leadership.

[40] Paul Bucala and Marie Donovan. "A New Era for Iran's Military Leadership"…

[41] Although the Ukrainian situation persists, it is hard to argue that after five years the current status quo will be overturned.

quoting the Emir of Qatar as praising Iran and Hamas were posted to Qatari media websites. These news articles were rapidly followed by a storm of new twitter accounts within *Council* states calling for a blockade of Qatar. Responsibility for these actions is unclear however some sources attribute this cyber-attack to Iranian actors.[42] Similarly, Yemen was in negotiations with the *Council* for membership however this has been stalled by the civil war (partially caused by *Council* involvement in Yemeni politics) which has been sustained by Iranian support to the Shia dominated *Houthis* rebels fighting the Saudi supported government forces.

Risks and Conclusion

The widespread adoption of hybrid warfare holds greater risk for Iran than Russia. The continued low intensity nature of hybrid warfare has the potential to flare up out of control of local participants and to lead to a major regional or international conflict.[43] Unlike Russian involvement in the Ukraine, whose government was already in turmoil, the Persian Gulf and greater Middle East have a large number of military forces capable of intervening; something that Iran's strapped conventional forces may be hard pressed to counter. By using hybrid capabilities, especially cyber capabilities, Iran runs the risk of another state or state affiliated group responding in kind. Despite these risks, the successful Russian campaign in the Ukraine offers Iran a model to extend its influence throughout the region. Like Russia, Iran has significant experience in the use of irregular warfare and cyber warfare. Similarly, Iran has geographic features that allow it to reduce its threat axis and hinder the flow of support to states in the region via A2/AD capabilities.

---

[42] Trey Herr and Laura K. Bate. "The Iranian Cyberthreat Is Real." *Foreign Policy*, last modified 26 July 2017, http://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real.

[43] Hall Gardner,"Hybrid Warfare…", 14.

Iran has two significant limitations if it wants to execute hybrid campaigns as successfully as Russia's Ukraine campaign. Iran's ability to win the information war by socially influencing its own citizen and external parties is limited and Iran will have a harder time building popular support and neutralizing opposition support. Iran's fractured command arrangements have limited its ability to plan, command and conduct a coordinated campaign across the various domains within hybrid warfare. The Iranian government and military do not have a tight working relationship, with political influence trumping a well-defined command structure. Iran appears to recognize these limitations and has taken recent steps to address the problem by reorganizing its general staff.

Hybrid warfare offers both Russia and Iran the ability to expand their regional influence despite weak economic outlooks limiting the recapitalization of their conventional forces. I anticipate that the success of Russia's campaign in Crimea will led to further campaigns by both Russia and Iran.

Bibliography

US Army Asymmetric Warfare Group. Russian New Generation Warfare Handbook. Fort Meade, MD: Department of Defence, 2016.

Alaaldin, Ranj. “How Will Iraq Contain Iran's Proxies?” The Atlantic, last modified 22 February 2018, https://www.theatlantic.com/international/archive/2018/02/the-man-who-could-help-rebuild-iraq/553799.

Anderson, Collin and Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage, and Revenge. Washington: Carnegie Endowment for International Peace, 2018.

Baezner, Marie and Patrice Robin. Cyber and Information warfare in the Ukrainian conflict. Zurich: Center for Security Studies, 2017.

Bucala, Paul. “Iran’s New Way of War in Syria,” American Enterprise Institute and the Institute for the Study of War, 2017. Last Accessed 12 May 2018, http://www.understandingwar.org/sites/default/files/Iran%20New%20Way%20of%20War%20in%20Syria_FEB%202017.pdf.

Bucala, Paul, and Marie Donovan. “A New Era for Iran's Military Leadership”. Last modified 1 December 2016, https://www.criticalthreats.org/analysis/a-new-era-for-irans-military-leadership.

Center for Strategic and International Studies, “Fateh-110,” Last modified 8 September 2016. https://missilethreat.csis.org/missile/fateh-110.

Condra, Jon. Business Risk Intelligence Decision Report 2017 End of Year Update. Flashpoint, 2017.

de Hass, Marcel. Russia's Military Reforms: Victory after Twenty Years of Failure. The Hague: Netherlands Institute of International Relations, 2011.

Deep, Alex. Balance Of Power, Balance Of Resolve: How Iran Is Competing With The United States In The Middle East. Last modified 12 January 2018, https://mwi.usma.edu/balance-power-balance-resolve-iran-competing-united-states-middle-east.

Director of National Intelligence. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Washington: U.S. Government Printing Office, 2018.

Eisenstadt, Michael. Iranian Military Power: Capabilities and Intentions. Washington, DC: The Washington Institute for Near East Policy, 1996.

Gardner, Hall. "Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict." Research Paper 123, NATO Defence College (December 2015): 1-16.

Grätz, Jonas. "Russia's Military Reform: Progress and Hurdles." CSS Analyses in Security Policy (Center for Security Studies), no. 152 (April 2014): 1-4.

Gunzinger, Mark. "Outside-In: Defeating Iran's Anti-Access and Area-Denial Threat." Last modified 20 January 2012, https://csbaonline.org/uploads/documents/Outside-In-Backgrounder.pdf.

Hashim, Ahmed S. "The Iranian Military in Politics, Revolution and War, Part Two." Middle East Policy Council XIX, no. 3 (Fall 2012): 65-83. Last accessed 20 May 2018, http://www.mepc.org/iranian-military-politics-revolution-and-war-part-two.

Herr, Trey and Laura K. Bate. "The Iranian Cyberthreat Is Real." Foreign Policy, last modified 26 July 2017, http://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real.

Keck, Zachary, "Meet Iran's "Carrier Killer": The Khalij Fars," Last modified 11 May 2013, https://thediplomat.com/2013/05/meet-irans-carrier-killer-the-khalij-fars/.

Larrabee, F. Stephen. "Russia, Ukraine, and Central Europe: The Return of Geopolitics," Last modified 15 April 2010, https://jia.sipa.columbia.edu/russia-ukraine-and-central-europe-return-geopolitics.

Mazzetti, Mark and Thomas Shanker. "Arming of Hezbollah Reveals U.S. and Israeli Blind Spots." New York Times, 19 July 2006.

McInnis, Matthew, "The Strategic Foundations of Iran's Military Doctrine," in Gulf Security after 2020, 5-11. London: The International Institute for Strategic Studies, 2017.

Missile Defence Advocacy Alliance, "Fateh-313", Last modified 3 March 2017, http://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/iran/fateh-313.

Nocetti, Julien. Guerre de l'information : le Web Russe. Paris : Centre des études de sécurité and Conseil Supérieur de la Formation et de la Recherche Stratégiques, 2015.

O'Connor, Tom. “U.S. Soldiers under Threat As Iran Allies Join Iraq Military with Plans to Kick Americans Out.” Newsweek, Last modified 9 March 2018, http://www.newsweek.com/us-soldiers-under-threat-iran-allies-join-iraq-military-kick-americans-out-839255.

Office of Naval Intelligence. Iranian Naval Forces: A Tale of Two Navies. Washington: Department of Defence, 2017.

Oliker, Olga. Russia's Chechen Wars 1994-2000. Santa Monica, CA: RAND Corporation, 2001.

O'Rourke, Ronald. "The Tanker War." Proceedings Magazine, May 1988. Last Accessed 10 May 2018, https://www.usni.org/magazines/proceedings/1988-05/tanker-war.

Peniston, Bradley. “The Day Frigate Samuel B. Roberts Was Mined”, Last updated 22 May 22 2015, https://news.usni.org/2015/05/22/the-day-frigate-samuel-b-roberts-was-mined.

Ruhe, Jonathan and Blake Fleisher. "Iran's Close Encounters with the U.S. Navy in the Persian Gulf." The National Interest, September 21, 2016.

Secretary of Defence. Unclassified Report on the Military Power of Iran 2010. Washington: Department Of Defence, 2010.

Seffers, George. "Russia, Iran and North Korea Bolder in Cyber Realm." Signal, 13 February 2018, https://www.afcea.org/content/russia-iran-and-north-korea-bolder-cyber-realm.

Waehlisch, Martin. "The Iran-United States Dispute, the Strait of Hormuz, and International Law." Yale Journal of International Law 37 (2012): 22-24.

Williams, Ian. “The Russia – NATO A2AD Environment”. Last modified 3January 2017, https://missilethreat.csis.org/russia-nato-a2ad-environment.

Zisse, Eyal. "Iranian Involvement in Lebanon." Military and Strategic Affairs 3, no. 1 (May 2011): 3-16.