Hybrid Warfare

Research into Hybrid Warfare

Josh Martin

Index

Introduction

A current problem with hybrid warfare and hybrid threats is that nobody can seem to agree upon on specific definition, which present a problem within itself. The European Centre for Excellence for countering Hybrid Threats defines hybrid threats as:

> “an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states’ and institutions’ vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.”

Whereas the U.S. Army defines hybrid threats and warfare as:

> “the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefiting effects" (Anderson, 2018)

Then the Chinese military and government do not have a current definition for hybrid warfare to my knowledge. They simply lump it into their strategy for constant unrestricted warfare. Unlike the Western idea of unrestricted warfare where we tend to think of it as salt the earth or glass an entire region with overwhelming military power, the Chinese government looks at unrestricted warfare where they use any facet of a society to combat their enemy. Whether that be diplomatic warfare, information warfare, traditional kinetic warfare, economic warfare, financial warfare, cyber warfare, lawfare, or any number of other facets in a society.

Breakdown

Hybrid warfare and hybrid threats present a huge threat that has not been dealt with by very many nations and is extremely hard to combat. Many factors in hybrid warfare present the same problems as many of forms of warfare outside of traditional kinetic warfare, a standard army cannot effectively combat or many times even see things like economic warfare or lawfare happening right in front of their eyes, mainly because that is out of the scope of their responsibilities. Economic warfare for example cannot be fought off with overwhelming military force, if you inflate or deflate the U.S. dollar by a certain percentage, you might not be able to effect the U.S. in any meaningful way, but you could crash the economy of a small country such as Guatemala, and this would be extremely hard to see and combat as or before it happens. Another large problem presented by this type of warfare is attribution, if you cannot figure out who your enemy is, it makes it a lot harder to fight them. For example, in October of 2019, articles started appearing that hard titles such as, "Russian Hacker Group Disguises Self as Iranian Hacker Group," it turns out that the Russian attributed hacker group known as Turla, hacked an Iranian-sponsored hacker group known as OilRig. Turla then used OilRig's servers, tools, and behavior to masquerade as them while carrying out various cyber operations. (Gatlan, 2019)

Though large terrorist and criminal organizations such as Daesh, Al-Qaeda, Solntsevskaya Bratva, or the Russian Business Network can conduct hybrid warfare in a more limited manner, it will be more common with the resources at the disposal of nation states. With the seemingly draw done of the wars in the Middle East, and the possibility of a regional conflict between nations such as China and Taiwan or Saudi Arabia, Israel and Iran growing larger, hybrid warfare, or as Russia refers to it as new generation warfare looks like more like reality. The Mobilizing Insights in Defense and Strategy Challenges for 2020-2021 lists hybrid warfare and threats as one of the challenges the Department of National Defence faces and states that:

"We are seeing a resurgence of strategic competition between states, which is unfolding daily through coordinated hostile activities across all spheres of state power (i.e., diplomatic, economic, information, military) that are deliberately crafted to fall below the traditional threshold of armed conflict. In this environment, there is a broader and "greyer" spectrum of threats with which governments and their military forces must contend, often with significant ambiguity and, policy and legal frameworks that have not kept pace with evolving threats." (Government of Canada, 2020)

Looking at this from the perspective of cybersecurity in Canada, if a nation or group were to implement hybrid warfare against Canada with cyber warfare or information warfare as a part of it, it will put a large amount of security professionals in an predicament where they are combating the full or at least targeted weight of a cyber-attack from a professional group. If for example this was someone like Russia, Iran, or China, that would be incredibly difficult to combat, especially if they possess the ability to replicate and repeat the 2.54 Tbit/s DDOS attack that Google suffered from in 2017. (Cimpanu, 2020)

Examples

Russian-Georgian War 2008

Kinetic Military Operations

The Russian-Georgian war took place in August of 2008, and was a part of two longer lasting conflicts in the region, the Abkhaz–Georgian conflict and Georgian–Ossetian conflict, which both had started in late 1989 and carry on to this day. Russian troops as part of a joint peace keeping force had been operating in the North and South Ossetian regions in order to keep the peace between Ossetian and Georgian forces. From August 1st to August 6th, 2008, relations between Georgian and Ossetian forces deteriorated rapidly after multiple bombings, and shootings targeting either side.

On August 7th, Georgian military forces began building up on the border. According to Russian peacekeeping forces, Georgian artillery fired artillery into the village of Khetagurovo located in South Ossetia. Later that day according to Georgian forces Ossetian forces destroyed a Georgian armored vehicle using a rocket propelled grenade, killing multiple Georgian troops. Both of these claims are heavily disputed by either side, and a ceasefire was agreed to later in the day.

Late August 7th early August 8th, a large contingent of Russian, North Ossetian, and South Ossetian forces and military hardware amassed at the border between South Ossetia and Georgia. Early morning on August 8th, Georgian forces launched an attack into South Ossetia against the South Ossetian forces. Later that morning, Russian and North Ossetian forces intervened, launching an attack on Georgia. Russian forces quickly gained air superiority within South Ossetia. Later in the week, Russia deployed troops from the battle gardened 58th Army, as well as Chechen, and GRU special operations units to South Ossetia to reinforce the peacekeeping troops already there and would later push into Georgia. Between August 8th and August 12th, the conflict between Russia, North Ossetia, South Ossetia, and Georgia raged on with Russia conduct multiple airstrikes far into Georgia, and Russia occupying a large region of Georgia just South of South Ossetia. On August 11th, three divisions of Russian naval troops, two battalions of Russian Marines, and forces from Abkhazia pushed into a region of North East and South of Abkhazia, occupying both regions. At the same time, ships from Russia's Black Sea Fleet decimated the Georgian navy after Georgian ships entered a Russian declared security zone.

On August 12th, the president of France negotiated a ceasefire and peace deal between all involved parties and the war officially ended. To this day, Russia occupies South Ossetia, Abkhazia, and the regions it took during the war.

Cyber Operations

- On July 20th, 2008, a few weeks before the official start of the Russian-Georgian war, multiple Georgian government websites were either defaced or completely taken down. (White, 2018)
- On August 7th, 2008 reports stated that multiple Georgian state servers and computers were under the control of an external threat group, being attributed to either Russian Intelligence agencies or the Russian Business Network, a criminal organization with close ties to the Russian Government and Russian President Vladimir Putin. (Danchev, 2008)
- August 8th, large scale DDOS attacks, and website defacements began against Georgian State targets. It was also reported that the majority of internet traffic in and out of Georgia had been routed through Russia and Turkey, effectively censoring traffic, and internet communication in and out of Georgia. (Danchev, 2008)
- Between August 9th and August 14th, multiple other attacks including DDOS attacks, defacements, and editing of news sites had taken place.

Analysis

Before and during the Georgian-Russian war, Russian military forces, intelligence agencies, and criminal organization attributed to the Russian government launched a coordinated cyber, information and military operation against Georgia. Russia effectively combined cyber, information and traditional warfare in the first large scale example of hybrid warfare. Proving to Putin and other nations that hybrid warfare is/was the future of warfare and that Russia was currently leading in the field. An interesting note is that Russia does not refer to this type of warfare as hybrid warfare, they call it new generation warfare and define it more closely to the Chinese definition of unrestricted warfare which can use any and all facets of a society or nation to conduct war rather than the Western definition for hybrid warfare.

Israeli-Iranian Conflict/s

Introduction

The current day conflicts between Israel and the countries and groups that surround it have been going on since modern day Israel's inception. The most sophisticated of these conflicts are the engagements between Israel, Iran, and Iranian proxies, though the official start of this is debated, it is generally agreed to be between a 1980-1985. There are too many events during this conflict to cover in this assignment, so I will try to cover the more significant or interesting ones.

Kinetic Events

- Throughout this conflict, Israeli forces have allegedly conducted dozens on targeted killings on Iranian officials and Iranian backed proxies. Some of these targets being:
    - Between 2010 and 2012, the Israeli intelligence agency Mossad allegedly killed four Iranian nuclear scientists and attempted to kill a fifth but failed.
    - In 2012, Mossad allegedly killed the Iranian general in charge of Iran's ballistic missile system and ballistic missile defense systems.
- Between June 25th, 2020 and July 19th, 2020, twelve targets in Iran suffered from mysterious explosions. The attacks have been attributed to Israel, but nothing has been confirmed or admitted to. There seems to be dispute on whether the explosions were caused by Israeli forces on the ground in Iran, or some sort of cyberattack. The attacks were at the following locations:
    - Parchin military facility
    - Shiraz power plant
    - Sina At'har health center in Tehran
    - Natanz nuclear enrichment facility
    - Shahid Medhaj Zargan power plant
    - Karun petrochemical center
    - Baqershahr oxygen factory
    - Multiple explosions in Tehran that Iran denies having happened.
    - Tondgooyan petrochemical plant
    - Mashad industrial complex
    - Ahvaz oil pipeline
    - Isfahan power plant
- During the 2006 Lebanon-Israel war, Iranian Revolutionary guard forces fought and trained alongside Hezbollah forces against Israel. Note that Hezbollah is allegedly funded and supported by Iran. One fact to support this claim is when the Iranian general, Kassem Soleimani was killed by a United States drone strike in early 2020, one of the other people killed in the strike was Abu Mahdi al-Muhandis, who is the former Secretary General of Hezbollah, and the flight they were both coming off of was coming from Lebanon. Also, during the Lebanon-Israel was, both Soleimani and al-Muhandis were on the ground in Lebanon.
- On November 18, 2020, Israel conducted strikes on Iranian military facilities located in Syria after Israel found explosives in the Israeli occupied Golon Heights region that were believed to be from Iran. (The BBC, 2020) (The only reason this is here is because it appeared at the time of writing this)

Non-Kinetic Events

- Alleged joint United States, Israeli cyberattack using Stuxnet on Iranian nuclear centrifuges.
- Iran cyberattack on Israel’s water supply. (Reuters, 2020)
- Cyberattack on Iranian Shahid Rajaee port (FRANTZMAN, 2020)
- Static Kitten attempted ransomware attack against Israeli organizations (Times of Israel, 2020)

Analysis

Though not a traditional war the Israel-Iran conflict is more akin to the US-USSR Cold War. Despite not being a hot war, or single event, both nations are using a complex mixture of traditional warfare, economic warfare, proxy groups, cyber warfare, information warfare, and lawfare to wage a long term hybrid war against each other.

Mitigation Methods

Mitigating and counteracting hybrid warfare and hybrid threats is no simple task. Raw military power alone cannot fight off a hybrid threat or spot it in most cases before it happens. A hybrid threat requires a multi-domain solution in order to find, deter, and mitigate the effects of these threats. In March of 2019, the Multinational Capability Development Campaign project released a paper on hybrid warfare and hybrid threats. This was the framework they released on how to counter these threats:

- **"Detect.** This component addresses the problem of detecting hybrid threats or attacks in the first place. It requires updating warning intelligence to monitor 'known unknowns' through indicators and warnings and discovering 'unknown unknowns' through pattern recognition and anticipation.
- **Deter**. This component addresses the deterrence of hybrid aggressors – or 'hybrid deterrence'. Deterring hybrid aggressors can be done, but it requires building on traditional deterrence to pursue credible measures through creative horizontal escalation, tailored and communicated to the aggressor, that are balanced between deterrence by denial – including resilience – and punishment.
- **Respond.** This component addresses how to respond to hybrid threats or attacks and offers a framework for doing so. The decision to respond by implementing appropriate actions and measures can be taken at any stage in the hybrid threat cycle, from identifying potential vulnerabilities that require resilience-building activity to punitive measures taken in response to a hybrid attack." (Multinational Capability Developement Campaign, 2019)

Summary

Though hybrid warfare, like most things, has been around since warfare has existed, in recent years it has been renewed to adapt to the worlds ever changing situation. Hybrid warfare is extremely hard for traditional militaries to fight due to its multi-domain approach than usually extends beyond the scope of military within the elements of national power. Starting in 2008, Russia really pioneered the way for modern hybrid warfare and is extremely affective at it but referring to it as new generation warfare rather than hybrid warfare. Due to hybrid warfare's multi-domain approach to warfare, there is no one way to combat it, especially since it is like the LEGO with warfare. Every country or group is going to build something different and will present their own unique and complex challenges.

References

Anderson, G. (2018, 02 12). *COUNTER-HYBRID WARFARE: WINNING IN THE GRAY ZONE*. Retrieved from Smallwarsjournal.com: https://smallwarsjournal.com/jrnl/art/counter-hybrid-warfare-winning-gray-zone

Bachmann, A. D.-D. (2019, June 17). *What is hybrid warfare and what is meant by the grey zone*. Retrieved from https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841

Bagge, D. P. (2019). *Unmasking Maskirovka Russia's Cyber Influence Operations.* Defense Press.

Brigadier (retd.) Ben Barry, S. M. (2019, March 4). *Countering Hybrid Warfare: a multinational approach*. Retrieved from IISS.org: https://www.iiss.org/events/2019/03/countering-hybrid-warfare#:~:text=The%20Countering%20Hybrid%20Warfare%20project,Norwegian%20Institute%20for%20International%20Affairs.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Harvard University Press.

Cimpanu, C. (2020, October 16). *Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date*. Retrieved from ZDNet.com: https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

Conley, H. A. (2016, October 6). *Kremlin Playbook.* Retrieved from CSIS.org: https://www.csis.org/analysis/kremlin-playbook

Cordesman, A. H. (2019, June 13). *The Strategic Threat from Iranian Hybrid Warfare in the Gulf*. Retrieved from CSIS.org: https://www.csis.org/analysis/strategic-threat-iranian-hybrid-warfare-gulf

Cordesman, A. H. (2020, August 18). *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*. Retrieved from CSIS.org: https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations

Cummins, S. T. (2019). *The Ultimate Art of War A Step-by-Step Illustrated Guide To Sun Tzu's Teachings.* Watkins Media Limited.

Danchev, D. (2008, August 11). *Coordinated Russia vs Georgia Cyber Attack in Progress*. Retrieved from ZDNet.com: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Deep, A. (2015, 02 03). *Hybrid War: Old Concepts, New Techniques*. Retrieved from Smallwarsjournal.com: https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques

Devost, M. (2018, May 25). *Putins Cyber OODA Loop is tighter than yours.* Retrieved from www.oodaloop.com: https://www.oodaloop.com/ooda-original/2018/05/25/putins-cyber-ooda-loop-is-tighter-than-yours/

Donghui Park, J. S. (2017, October 11). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.* Retrieved from jsis.washington.edu: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Dorogan, A. S. (2010). *The New Nobility The Restoration of Russia's Security State and the Enduring Legacy of the KGB.* PublicAffairs.

Fireeye. (2014, October 27). *A WINDOW INTO RUSSIA'S CYBER.* Retrieved from Fireeye.com: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

FRANTZMAN, S. J. (2020, October 22). *Iran's 'Quick Sand' cyberattack on Israel by 'MuddyWater' revealed*. Retrieved from The Jerusalim Post: https://www.jpost.com/middle-east/irans-quick-sand-cyberattack-on-israel-by-muddy-water-revealed-646583

Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicization.* Oxford University Press.

Gatlan, S. (2019, October 21). *Russian Hackers Use Iranian Threat Groups Tools, Servers as Cover*. Retrieved from Bleepingcompute.com: https://www.bleepingcomputer.com/news/security/russian-hackers-use-iranian-threat-groups-tools-servers-as-cover/

Government of Canada. (2020, 01 06). *MINDS Policy Challenges 2020-2021*. Retrieved from Government of Canada: https://www.canada.ca/en/department-national-defence/programs/minds/defence-policy-challenges.html

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Anchor.

Karber, D. P. (2018, 04 26). *VIDEO: DR. PHILLIP KARBER ON UKRAINE AND THE RUSSIAN WAY OF WAR*. Retrieved from Modern War Institute: https://mwi.usma.edu/video-dr-phillip-karber-ukraine-russian-way-war/

Lind, W. S. (1985). *Maneuver Warfare Handbook.* Routledge.

McReynolds, J. (2015). *China's Evolving Military Strategy.* Jamestown Foundation.

Michael Connell, S. V. (2017, March). *Russia's Approach to Cyber Warfare.* Retrieved from www.cna.org: https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

Mitrohhin, C. A. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB.* Basic Books.

Mitrokhin, C. A. (2018). *The Mitrokhin Archive: The KGB in the World.* Penguin Press.

Multinational Capability Developement Campaign. (2019, March). *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*. Retrieved from https://assets.publishing.service.gov.uk:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Perry, B. (2015, 08 24). *NON-LINEAR WARFARE IN UKRAINE: THE CRITICAL ROLE OF INFORMATION OPERATIONS AND SPECIAL OPERATIONS*. Retrieved from smallwarsjournal.com: https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera

Pindják, P. (2014, November 18). *Deterring hybrid warfare: a chance for NATO and the EU to work together?* Retrieved from NATO.int: https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html

POMERANTSEV, P. (2014, May 5). *How Putin Is Reinventing Warfare*. Retrieved from foreignpolicy.com: https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/

Reuters. (2020, May 18). *Israel linked to cyberattack on Iranian port: Washington Post*. Retrieved from Reuters.com: https://www.reuters.com/article/us-mideast-iran-israel-cyber-idUSKBN22U363

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux; Illustrated edition.

Sawyer, R. D. (2007). *The Tao of Deception: Unorthodox Warfare in Historic and Modern China .* Basic Books.

Sexton, M. (2020). *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization.* Independently published.

The BBC. (2020, November 18). *Israel strikes 'Iranian military sites' in Syria after bombs found in Golan*. Retrieved from bbc.com: https://www.bbc.com/news/world-middle-east-54985861

The European Centre for Excellence for countering Hybrid Threats. (n.d.). *Hybrid Threats as a Phenomenon*. Retrieved from hybridcoe.fi: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Thomas, T. L. (n.d.). *Nation-State Cyber Strategies: Examples from China and Russia.* Retrieved from ndupress.ndu.edu: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850

Times of Israel. (2020, October 16). *Cybersecurity groups: Iranians targeted top Israeli firms in ransomware attack*. Retrieved from Time of Israel: https://www.timesofisrael.com/cybersecurity-groups-iranians-targeted-top-israeli-firms-in-ransomware-attack/

White, S. P. (2018, March 20). *understanding-cyberwarfare-lessons-russia-georgia-war.* Retrieved from mwi.usma.edu: https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/

Xiangsui, Q. L. (2017). *Unrestricted Warfare.* Shadow Lawn Press.

Żaryn, S. (2019, August 9). *Russia's hybrid warfare toolkit has more to offer than propaganda*. Retrieved from defensenews.com: https://www.defensenews.com/opinion/commentary/2019/08/09/russias-hybrid-warfare-toolkit-has-more-to-offer-than-propaganda/