Hybrid Warfare Tactics

POL61305: Emerging Technologies and International Security

Author redacted

May 22, 2020

This literature review aims to survey the broad range of tactics that can be used when waging hybrid warfare, and to provide the reader with real world examples of their usage.

It identifies seven different hybrid tactics (political warfare, information warfare, conventional warfare, proxy warfare, cyber warfare, lawfare and economic warfare) and points to multiple case studies where actors such as Russia, China, The United States, Iran and others engage in hybrid wars.

1 Introduction

As defined by Weissman, hybrid warfare concerns active measures taken by one actor towards another actor [1]. The dynamic nature of hybrid warfare means that it is not a static repertoire of techniques and tactics, but rather an ever changing mélange of actions tailored towards a specific situation against a specific adversary [2], often with the intention of shifting the (Clauswitzian [3]) center of gravity for the conflict away from the military domain and into other domains.

This literature review aims to list the different tactics that have been used in hybrid wars. It does so by outlining categories of hybrid tactics and referencing documented case studies for each. In order to profile the full range of hybrid tactics, the "definitional net" of hybrid warfare is cast deliberately wide to encompass as much of the phenomenon as possible as suggested by Wither [4].

2 Political warfare

Political warfare is defined by Lord to be "a general category of activities that includes political action, coercive diplomacy and covert political warfare" which often takes place on ideological the level [5, p.322, 34], and by Galula to be "when politics becomes an active instrument of an operation" [6]. Examples include organizing protests (e.g. Russia and Estonia's 'Bronze Soldier' incident [5, p.89]), funding of foreign political and religious organizations (e.g. Iran funding Shi'a militias which often mature into outright political actors themselves [5, p.89]), and influencing grassroots political opinion aboard (e.g. the use of social media by ISIS [5, p.190]).

2.1 Electoral intervention

On particularly pertinent form of political warfare is electoral intervention, where one party attempts to influence the democratic election process of another. Conventional methods of electoral intervention revolve around manipulating electoral registrations & vote counting (such as occurred in Zimbabwe by private Israeli firms [7]), but more recent methods aimed at influencing the opposition have emerged, particularly by Russia [8; 9]. These methods have now gained the attention of NATO as a threat of a severity capable of eliciting a response [10].

3 Information warfare and propaganda

Information warfare in an overloaded term, but here refers to a confrontation in the information space in order to undermine the political, economic and social system and effect massive brainwashing of the population, and is known in Russia as *reflexive control* [11]. The idea is that an opponent should be manipulated into voluntarily choosing an action that is desired by the aggressor [12]. It includes denial of involvement by the aggressor, concealing aggressive actions, obfuscating goals and retaining plausible deniability and legality [13].

4 Conventional warfare

Conventional warfare is war fought conventional forces (without chemical, biological or nuclear weapons) [14], and NATO defines a 'hybrid threat' to include both conventional and non-conventional means [15]. As Galeotti says, hybrid warfare aims to utilize conventional tools as little as possible, and uses other tactics listed to ensure that it takes place on the best terms possible [16, p.165]. In the recent hybrid war between Russia and Ukraine, 'little green men' (soldiers without insignia) were used by Russia to project military force (backing up Ukrainian separatists who were officially doing the fighting) with plausible deniability [17; 18].

5 Proxy warfare & Extremism

Proxy warfare is defined by Mumford as the "indirect engagement in a conflict by a third party wishing to influence its strategic outcome" [19], and as such has a nebulous definition that could include other tactics listed here depending on what forms of fighting are taking place (as shown by Marshall's recent examples [20]).

One notable example is the Iranian Quds Force, which supports proxy groups such as Hezbollah in the Middle East [21; 22], and is an active sponsor of terrorism [23]. Terror-like actions are used extensively by Iran to project power; CSIS describes a recent incident where oil tankers in the Gulf of Oman were attacked, and outlines the range of possible threats that Iran can use in the region, from mines to ad-hoc craft with explosives [24].

6 Cyber warfare

Lucas Kello says that cyber warfare is a good fit for hybrid warfare since it allows aggressors to harm adversaries below the level that would typically elicit a response. In fact, it is so endemic in the 21st century, that he coined the term 'unpeace', in recognition of it being so commonly used between hybrid actors that it is almost constant [25]. Recent examples of cyber warfare include the Stuxnet worm which targeted Iranian nuclear reactors [26], sabotage of a country's digital health infrastructure (such as Wanna Cry in 2017 [27]), and Russia's attacks against Estonia, Georgia and Ukraine [11; 28; 29; 30].

7 Lawfare

Lawfare is defined by Dunlap as "the strategy of using or misusing law as a substitute for traditional military means to achieve an operational objective" [31], who reasons that lawfare has emerged as an increasingly viable strategy as international law and globalization have made the legal judgment of actions more important (especially in democracies, where support for wars is based on public support).

Kittrie breaks lawfare down into two classes; *instrumental lawfare* which are legal tools used to achieve the same goals as armed conflict would (such as asserting territorial claims over land rather than invading it directly), and and *compliance-leverage disparity lawfare*, which is used on the kinetic battlefield and gives an advantage to actors who ignore the law over those that are compelled to follow it (such as by ignoring rules of engagement) [32].

8 Economic warfare

Economic warfare is the use of financial and business oriented mechanisms to harm an adversary, and includes the use of sanctions, destabilisation of energy prices, transnational crime, preclusive purchasing and other similar means [33; 34]. These methods can be tightly aimed at specific targets, but are commonly applied in a manner that quickly pervades the whole of a society, and can deal psychological damage on a population-wide basis [35].

Most recent usages of economic warfare are associated with China, such as strategically buying foreign ports to gain leverage over trade and intelligence insights [36], and subsidizing Huawei in order to gain marketshare (and thus significant soft and hard power) in the international 5G market [37; 38].

9 Conclusions

This literature review has outlined seven distinct tactics used to wage hybrid warfare and outlined examples of each. The review shows the breadth of possible threats involved when actors utilize the tactics of hybrid warfare, and as such, underscores the breadth of the response required to effectively counter a hybrid adversary.

Further research is warranted to review possible counter measures that can be deployed against each of the above techniques. Surveying the broad landscape of hybrid tactics was prioritized over a deeper analysis of individual methods in this review, but further work could outline the suitability of each tactic listed above for use in different settings and against different adversaries.

References

[1] Mikael Weissmann. Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*, 5(1):17–26, 2019.

[2] Johann Schmid. Hybrid warfare on the ukrainian battlefield: developing theory based on empirical evidence. *Journal on Baltic Security*, 5(1):5–15, 2019.

[3] Carl Von Clausewitz. *On war*, volume 2. 1956.

[4] James K Wither. Making sense of hybrid warfare. *Connections*, 15(2):73–87, 2016.

[5] Linda Robinson et al. Modern political warfare: Current practices and possible responses, 2019.

[6] David Galula. *Counterinsurgency warfare: theory and practice*. Greenwood Publishing Group, 2006.

[7] Greg Mills. The african security intersection. 2020.

[8] SG Jones. Russian meddling in the united states: The historical context of the mueller report. *CSIS Briefs*, 2019.

[9] William Carter. Csis election cybersecurity scorecard: The outlook for 2018, 2020 and beyond. 2018.

[10] Jean Paul Pierini. Election meddling, the'unnoticed'dissonance between'alarming warnings' and the reductive assessments about their'effects' on returns and the not-necessarily'foreign'media manipulation. *Rassegna della Giustizia Militare*, (6), 2019.

[11] Eve Hunter and Piret Pernik. *The challenges of hybrid warfare*. International Centre for Defence and Security, 2015.

[12] Timothy Thomas. Russia's reflexive control theory and the military. *Journal of Slavic Military Studies*, 17(2):237–256, 2004.

[13] Maria Snegovaya. Putin's information warfare in ukraine. *Soviet Origins of Russia's Hybrid Warfare', Russia Report*, 1:133–135, 2015.

[14] William E Gortney. Department of defense dictionary of military and associated terms. Technical report, Joint Chiefs Of Staff Washington, 2010.

[15] Scott Jasper and Scott Moreland. The islamic state is a hybrid threat: Why does that matter? *Journal Article| Dec*, 1(11):50pm, 2014.

[16] Pikulicka-Wilczewska Agnieszka and Sakwa Richard. Ukraine and russia: People, politics, propaganda and perspectives. *E-International Relations Publishing*, 121, 2015.

[17] Alexander Lanoszka. Russian hybrid warfare and extended deterrence in eastern europe. *International affairs*, 92(1):175–195, 2016.

[18] Frank Bekkers, Rick Meessen, and Deborah Lassche. *Hybrid conflicts: the new normal?* Den Haag: TNO, 2019.

[19] Andrew Mumford. *Proxy warfare*. John Wiley & Sons, 2013.

[20] Alex Marshall. From civil war to proxy war: past history and current dilemmas. *Small Wars & Insurgencies*, 27(2):183–195, 2016.

[21] Seth G Jones. *War by Proxy: Iran's Growing Footprint in the Middle East*. Center for Strategic & International Studies, 2019.

[22] Eitan Azani. The hybrid terrorist organization: Hezbollah as a case study. *Studies in Conflict & Terrorism*, 36(11):899–916, 2013.

[23] Daniel Byman. Iran, terrorism, and weapons of mass destruction. *Studies in Conflict & Terrorism*, 31(3):169–181, 2008.

[24] Anthony H. Cordesman. The strategic threat from iranian hybrid warfare in the gulf. 2019.

[25] Dennis Broeders. Mutually assured diplomacy: Governance,'unpeace'and diplomacy in cyberspace. *Digital Debates*, page 26.

[26] James P Farwell and Rafal Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[27] Anders Carlsson and Rune Gustavsson. The art of war in the cyber world. In *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, pages 42–44. IEEE, 2017.

[28] Madelena Anna Miniats. War of nerves: Russia's use of cyber warfare in estonia, georgia and ukraine. 2019.

[29] Adrian Victor VEVERA and Ella Magdalena CIUPERCĂ. The dimensions of cyber warfare in the sino-russian space, 2019.

[30] Henrik Praks. *Hybrid Or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics: the Case of Estonia*. Research Division, NATO Defense College, 2015.

[31] Charles J Dunlap Jr. Lawfare today: A perspective. *Yale J. Int'l Aff.*, 3:146, 2008.

[32] Orde F Kittrie. *Lawfare: Law as a weapon of war*. Oxford University Press, 2016.

[33] Kathleen Abbott. Understanding and countering hybrid warfare: Next steps for the north atlantic treaty organization. 2016.

[34] Marjorie M Farrar. Preclusive purchases: politics and economic warfare in france during the first world war. *The Economic History Review*, 26(1):117–133, 1973.

[35] NA Lambert, George Perkovich, and Ariel Levite. Brits-krieg: The strategy of economic warfare. *Understanding Cyber Conflict*, 14:123–146, 2017.

[36] Kristin Huang. Why China buying up ports is worrying Europe. `https://www.scmp.com/news/china/diplomacy/article/2165341/why-china-buying-ports-worrying-europe`, 2018.

[37] Kaan Sahin and Didi Tatlow. Berlin's preliminary 5g decision. 2019.

[38] Todd Davies. Emerging technologies and international security literature review: Conceptualizations of 5g. `https://todddavies.co.uk/api/notes-dl?key=5719549001334784`, 2020.

[39] Jean Baptiste Jeangène Vilmer and Paul Charon. Russia as a hurricane, china as climate change different ways of information warfare. *War on the Rocks*, 2020.