Past and Present Russian Information Operations in Ukraine: Competition into Conflict

Stephen Defibaugh
Marymount University, Arlington Virginia, USA

Stephen_Defibaugh@marymount.edu

Abstract: Sovereign nation-states seek to ensure the survival and advancement of national goals through cooperation, competition, and conflict. This paper explores the use of irregular warfare prior to and during the transition from competition to conflict as an international tool to assert control over public narratives. This stratagem has been made an increasingly effective tool through means of the Internet. Informational warfare is not a new concept, however, the precedent of operations in the information environment in concert with operations in the physical realm have started to take shape in the struggle between Ukraine and Russia over the past several decades. The visualization of the competition continuum model allows us to examine events and understand how actions taken in the cyber realm effect an informational narrative, and not simply be portrayed as a method of simple attack and defense.

Keywords: Cyber, Cyber warfare, Operations in the information environment, Ukraine, Russia

1. Introduction

The authority of states to govern themselves, commonly termed sovereignty, has been well established in history. One of the most notable periods in the establishment of sovereignty and nation-state rights is the Peace of Westphalia in 1864. This event ended the 30 Years War between the European countries of Spain, the Dutch Republic, the Holy Roman Empire, and Sweden (Britannica, 2023). As a part of the negotiated terms, countries were recognized in their right to govern territories which belong to them. This may be considered as one of the foundational points in history that establishes sovereign nation-state boards and the concept of states infringing upon that sovereignty as an act of aggression. Since the dissolution of the Soviet Union in 1991 with the Belavezha Accords, Ukraine has been a sovereign nation (Cosgrove, 2020). Since then Ukraine experienced much in the way of friction with the neighboring Russian Federation and the climate between the two countries has evolved from competition into outright large-scale conflict. For this comparison, the term Russia will be used to describe the post-Belavezha Accords dissolution of the Soviet Socialist Republics (USSR). To aid in the understanding of distinction between acts of national competition and acts of national conflict, the competition continuum model provides context based on observable events. The competition continuum model can also be used to better understand Information Operations campaigns to include not only military deception tactics but also public affairs outreach and attempts to influence the information environment from both competitors. Also seen is one of the first instances of cyber warfare operations being used in concert with forces in the physical realm.

2. Assumptions, Limitations, and Scope

A limitation of this research is that it is exploratory in nature and will only serve to essentially expose and explore a potential area in cyber security research. It will not be able to provide mitigations or corrections. The scope of this research will consist of cyber war and cyber warfare doctrine that would be executed at the nation-state level. As stated by Scott Applegate (2012), cyberspace appears to be more of a contested territorial domain that includes competitors from state and non-state domains, organized groups, proxies, and individuals. For the purposes of this research, cyber terrorism will not be in scope. As this is an exploratory research case, the substantive theory methodology was utilized from similar exploratory studies (Defibaugh, 2022).

3. The Competition Continuum

Competition between both friendly and adversary nations is an accepted aspect of international relations. According to the Chairman of the Joint Chiefs of Staff (CJCS) Joint Doctrine Note (JDN) 1-19, the competition continuum, “is the fundamental aspect of international relations” (Staff, 1998). Instead of attempting to forcibly contextualize global international relations into either peacetime or wartime, the Competition Continuum provides a model to understand the complex interplay between nations through enduring competition, cooperation, and conflict (Staff, 1998). Sovereign states seek to ensure the survival and the advancement of aims that support their growth and expansion. The aspects of this competition are advantages in diplomatic relations, economic resources, and strategic positions and capabilities or leverage enough to influence other sovereign nations towards a positive outcome. The continuum is a model to help frame the relationships by

generally categorizing them into cooperation, competition that is not armed conflict, and armed conflict. The competition continuum is distinct in that it is enduring and unceasing, though not necessarily linear or cyclical in nature. Though, this analysis will focus on the competition continuum between nation-states. It will not deeply examine the behaviors of cooperation or competition between business entities engaged in industrial, intellectual, or technological competition. As there has been a historically proven degree of tension politically, economically, and strategically between Ukraine and Russia, the cooperative spectrum of competition will not be examined as deeply. The basis of the comparative analysis will examine the events of 2014 with the events of the 2021 Russo-Ukrainian conflict. It will compare and contrast the chronological events that led out of competition and into crisis and armed conflict.

4. Escalation into Conflict

The 2014 escalation into open warfare began during the Crimean annexation. The change in national leadership left the sovereign nation in a weakened state and Russian military forces were deployed into Crimea through Novorossiysk (Cosgrove, 2020). During the buildup to the actual deployment of forces, multiple forms of coercion were taking place through diplomatic and military means utilizing political pressure and the propositioning of military forces (Cosgrove, 2020). Russia also took the opportunity to leverage its civil-military operations (CMO) apparatus and engage several pro-Russian non-governmental organizations (NGOs) to add additional pressure and destabilize the political environment. Russia also conducted informational campaigns to widen the distribution of pro-Russian sentiments and instill a sense of fear in the populations of Crimea and Russia by playing upon fears of ethnic restrictions and the limiting of citizen freedoms should an independent government in Ukraine become fully realized (Cosgrove, 2020). Irregular warfare operations continued when the leader of the Ukrainian government, Viktor Yanukovych, was overthrown and fled the country military intelligence assets were mobilized to secure strategic locations for Russia. Economic coercion was applied in the form of embargoes against Ukrainian food imports and exports. By the end of February, unmarked forces, later identified as Russian special operations forces (SOF) were deployed to secure Crimean government buildings to include the Supreme Council of Crimea. At this point, the puppet government of Crimea was dissolved and reformed to seek further sovereignty and independence from Ukraine. This was a clear move favoring Russian national strategy and ratcheting the pressure against the Ukrainian government and its citizens.

5. Present Escalations

Leading up to the 2021 armed conflict between Russia and Ukraine, it seemed that a very similar campaign was enacted in order to advance Russia's national objectives. Political, economic, information, and ultimately military force was leveraged in order to simultaneously destabilize Ukraine and legitimize Russian activities. However, this campaign distinguished itself from others in that the present conflict integrated Offensive Cyber Operations (OCO) as a component of the larger operations in the information environment (OIE). Rule 25 of the Tallinn Manual on the International Law Applicable to Cyber Warfare offers that the law of Armed Conflict does not expressly prohibit the use of cyber operations, though the nature of the conflict does have a bearing on how actions and effects will be perceived by the world as they are observed (Schmidt, 2013). Like the events in 2014, there were observable and reported uses of cyber operations as a part of OIE in a coordinated operational tempo (OPTEMPO) with military forces operating in the physical environment. Russia conducted distributed denial of service (DDoS) attacks and website defacements against Ukrainian instructions and media outlets in order to control a pro-Russian narrative while effectively degrading or outright denying Ukraine's ability to function as a effective government entity for it's citizens (Baezner, 2018). One of the differences in 2021 laid in the ability of Ukraine to conduct their own OIE, rather than purely defensive operations. Ukraine was able to leverage media platforms to include television and internet social media to push an alternative narrative (Debora, 2021). This alternate narrative, though, brings Ukraine into a state of irregular warfare as an active participant rather than a defensive target that is simply resisting aggressor operations in the information environment. Ukraine now strategically evaluated and applied leverage to the Russian centers of gravity in order to demoralize and degrade the will to continue engaging in both OIE and combat operations. Within this evolution of events we also observe a microcosm of evolution from competition into crisis and conflict by simultaneous surges and accelerations per Figure 1.

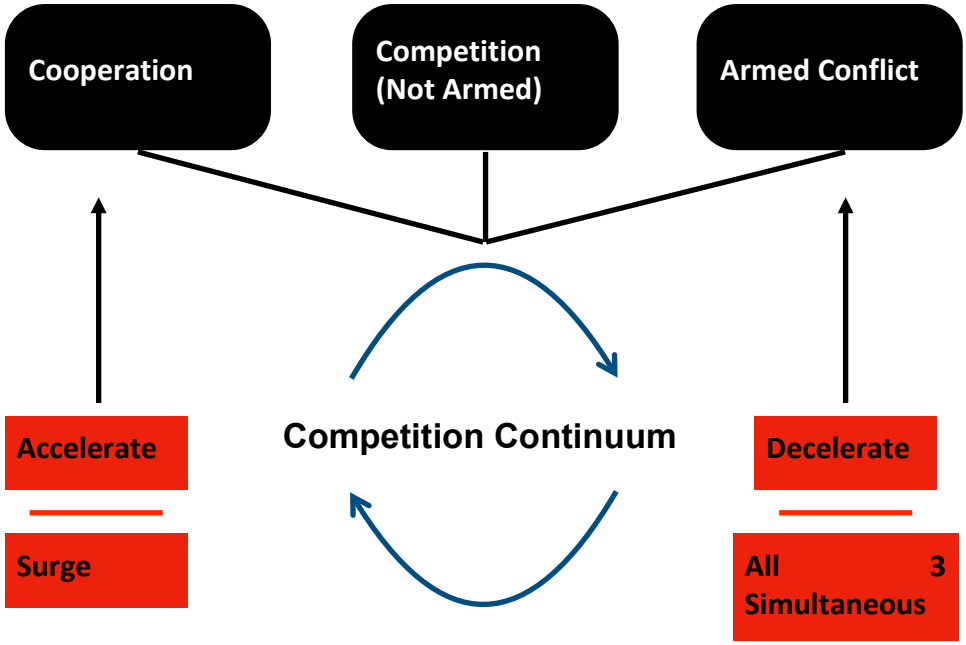

Figure derived from Joint Chiefs of Staff, Joint Doctrine Note 1-19 - Competition Continuum, 2

Figure 1: Competition Continuum Model

6. Conclusions and Future Areas of Research

Comparative analysis between the events of 2014 and 2021 demonstrate a clear repetition in tactics, techniques, and procedures (TTPs) utilized in both of the IO campaigns of Russia. The uses of coercion to conduct irregular warfare between the two sovereign nations clearly continued as well as operations in the information environment to justify the actions taken to the observing world (Doroshenko, 2021). Though both countries did conduct elements of cyber warfare as a part of campaign operations, Ukraine was able to popularize and legitimize their resistance against their Russian aggressors and rally significant support from external organizations and nations. Though the species of Information Operations was similar the employment of such operations had significantly different affects in 2021 than what occurred in 2014. We can we demonstrated the struggle for control of the narrative, especially in the control of economic and social sources of information. A review of current methodologies to identify the nuances in the shifts of the competition continuum may prove beneficial in determining what constitutes as irregular warfare and operations in the information environment and what actions constitute outright cyber warfare. Actions which are seen in the context of a single hostile conflict may, on a scale of global information operations, constitute attempts to gain leverage and coerce or maneuver other nation-states into unfavorable or untenable positions in order to cement an advantage. In a context of academic discussions, this is seemingly straight forward. Yet, when applied, the practices lack quantitative and qualitative rigor to hold up to the shifting complexities of global circumstances. One proposed area of research on this topic would be examining the potential interruption of international trade, either focusing on maritime or air freight. By manipulating international trade and supply, one nation could gain a significant advantage in leverage over another, though, attribution of this would be complicated by the use of the Internet to conduct potentially anonymous acts of competition by proxy. To more quickly identify potential competitors, a proposed area of study would be to examine the disruption of maritime shipping through the exploitation of cyber vulnerabilities and utilize the competition continuum to determine whom might potentially benefit from such aggression. By possibly accepting that cyber warfare can be viewed through a conventional lens but applied on differing scopes, scales, and speeds, we may gain some insight into further defining actions that constitute cyber warfare and actions that or in the cyber environment which support operations in the information environment.

References

Applegate, S.D., 2012, June. The principle of maneuver in cyber operations. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-13). IEEE.

Baezner, Marie. Cyber and Information warfare in the Ukrainian conflict. No. 1. ETH Zurich, 2018

Britannica, T. Editors of Encyclopaedia. "Peace of Westphalia." *Encyclopedia Britannica*, June 23, 2023. https://www.britannica.com/event/Peace-of-Westphalia.

Cosgrove, Jonathon. "The Russian invasion of the Crimean peninsula, 2014-2015: A post-cold war nuclear crisis case study." Applied Physics Lab, Johns Hopkins University Laurel Md Laurel (2020) 6-7.

Debora, Sabaria Catharin. 2021. "AN ANALYSIS OF ICT IMPACT ON UKRAINE AND RUSSIA CONFLICT". Journal of Social Political Sciences 2 (4), 398. https://doi.org/10.52166/jsps.v2i4.83

Defibaugh, S. and Schaeffer, D., 2022, March. Can Attrition Theory Provide Insight for Cyber Warfare?. In International Conference on Cyber Warfare and Security (Vol. 17, No. 1, pp. 55-62). Academic Conferences International Limited.

Doroshenko, L., & Lukito, J. 2021 Oct 28. Trollfare: Russia's Disinformation Campaign During Military Conflict in Ukraine. International Journal of Communication. [Online] 15:0

Joint Chiefs of Staff, *Joint Doctrine Note - Competition Continuum,* JDN 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), v-2, https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf

Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare, xiv-xx. Cambridge: Cambridge University Press, 2013.