Working Paper
SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION EU / EUROPE | WP NR. 03, JUNE 2023

The Absolute Ideal: Military Cyber Capabilities in War and Society

Mika Kerttunen

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Table of Contents

Executive summary

Does the employment of military cyber capabilities constitute war? How this question is answered is essential to the study of war; the development of military cyber doctrines, units, and education; and the intentional employment of state or military cyber capabilities against other states both in peacetime and war. Contemporary literature portrays cyber means as effective and considers cyber war or warfare as being waged. Legal theory and state position analysis thus follow the black letter of the law, especially focussing on whether the use of cyber capabilities constitutes the use of force or armed attack.

This research approaches the employment of military cyber capabilities from a military theoretical and operational perspective. The first part examines war as a concept and phenomenon and engages with military cyber thought. Departing from the key Clausewitzian maxims about war as a duel, violent, a play of chance, and rational through political subordination and intentionality, it argues that the employment of military cyber capabilities can constitute war in much the same way as any employment of destructive state or military capabilities. This conceptual and absolute claim, however, does not suggest that in every case of employment, determinations will end up with such an affirmative result.

The second part investigates how and for what purposes states have developed military cyber capabilities. It offers doctrinal, organisational, and operational insights guiding national development. It notes the diversity of thought and the variety of national capabilities ranging from network intelligence, destructive means, and, aside from doctrinal clarity, also information operations. Most importantly, few countries have the capacity to support combat operations with deployable cyber means. Espionage, subversion, and oppression seem to trump battlefield capacity.

The third part examines how various cyber capabilities have been used in the Russo-Ukrainian war. Based on empirical analysis of several information technology or cybersecurity companies, think tanks, databases, and individual experts, it observes that a wide range of cyber-attacks have been conducted without significant military operational benefit. It recognises how Russian intelligence and data-wiping attacks intensified before the conventional offensive and how Ukrainians have been able to defend and protect national data and connectivity-dependent services. Most of the destruction and civilian suffering have been caused by kinetic and explosive energy, i.e., ammunition, rather than by electromagnetic energy.

The conclusion calls for political and operational caution. As the employment of cyber capabilities can result in violent acts and can cause destruction, the use of military cyber capabilities runs the risk of escalating situations. Transparent and accountable national cyber governance and doctrinal reconsideration of the semi-independent status of the cyber operators are needed to rein in operations-and-punishment savvy cyber and security apparatus.

Introduction

War can and needs to be portrayed, approximated, and analysed in various ways. We can think war as a stage, a state of affairs, and a phenomenon; in the pursuit of knowledge, understanding, and explanation, we use terminology that is borrowed and transferred, conceptual or politically convenient, and legally-accepted or scientifically-precise.

This research paper asks whether the employment of cyber capabilities constitutes war as understood in theory of war. It examines classical and post-modern theories of war and cyber and information warfare, as well the practice of employment of cyber capabilities in the Russo-Ukrainian War in 2022.

The importance of answering these questions lies in the political, legal, and moral significance of war: responsibility, adherence to or violation of international law, the protection of persons and property, including data, and the conduct of online and offline operations. War as a practice of employing military cyber capabilities testifies to the separation and relationship of competencies/powers, a key qualitative feature of democratic and constitutionally-organised ways of societal and international life.

A careful reader should note that the military theoretical and operational study of war differs from the legal scholastic and normative study of, for example, the thresholds of on the use of force (UN Charter 2[4]) and armed attack (UN Ch. 51), the scope of the protection of property, and the legality of the means and methods of war.

Following Carl von Clausewitz's dualistic distinction between the absolute and real, Part 1, *Impressionism*, recognizes how the practices of understanding war are bound to remain incomplete, phenomenological impressions. [1] Moving from the conceptual notion of war to its concrete manifestations, this analysis expands the realm of war and assigns subsequent political, legal, and moral responsibilities to cyber activities which some states, politicians and operators wish to avoid. As both professional and academic cyber literature tend to usually adopt a rather lax reading of war, the literature exemplifying the development of academic and professional thought covers a variety of issues, threats, and solutions. Part 1 concludes by examining whether the tendencies of war are manifested in the employment of cyber capabilities.

While Part 1 relies primarily on theoretical considerations and deductive inference, Part 2, *Naturalism*, gauges the doctrinal and organisational development of military cyber capacity. By focusing on military cyber doctrines and units, it seeks to clarify how cyber capabilities can be used to support politico-strategic and military operational objectives. Here, two different schools of thought are identified. One school of thought recognises that armed forces and their capabilities, including cyber, support liberal democratic societies and values. In this framework, military cyber operations are conducted against external adversaries and enemies, alarmingly commonly in peacetime, but mainly in armed conflict and

[1] It is appropriate to note that, despite its heavily leaning on the German edition of *Vom Kriege*, this research does not claim to make *was eigentlich spracht* or should-have-thought an argument. By applying a Clausewitzian critical methodology that war, by its very nature, varies beyond easy recognition and that the absolute is always undermined by the real, the thesis for contemporary purposes merely seeks to stand on the shoulders of a giant. The inquiry is Clausewitzian, but its object is the nexus of war – military cyber capabilities.

war. In addition, the cyber-digital assets the defence sector possesses are used to support civilian authorities and processes in the event of an incident. The other school of thought considers the armed forces and their capabilities, including cyber, to support authoritarian/autocratic regimes against domestic and foreign threats. Here, military cyber capabilities are developed and deployed for oppressive and subversive, even criminal, purposes. In the first ideal model, powers are separated; in the second, power is often concentrated.

Part 3, *Expressionism*, explains the role and significance of military cyber capabilities in (interstate) war. The theoretical conclusions and doctrinal observations developed above are used to analyse the role of military cyber activities in a contemporary war. The section highlights the selection of Ukrainian targets which Russia has operated against in 2022 and examines the Russian actors who carried out these attacks. It discusses the alignment of cyber-attacks with conventional military advances and the strategic or military effects of the Russian cyber activities. It explains the Ukrainian ability to defend against, respond to, or recover from the attacks.

The conclusion, *Pointillism*, acknowledges the significant amount of politically-motivated and intentionally-destructive employments of cyber capabilities constituting violence and war. However, it segregates war as an absolute abstraction of such violent and similar activities from warfare as one more concrete way of approaching and understanding war. Cyber warfare as a concept and practice aligns with how war is understood in theories of war: forceful and fluid, directly and indirectly violent, intentional, and uncertain. The research finds how the understanding the employment of offensive cyber capabilities as war entails uneasy political, legal, and moral consequences decision-makers have refused to recognise.

The research also identifies a gap between Western perceptions on Russian military cyber prowess (high) and the actual significance of Russian cyber-attacks (low). It suggests several reasons for this misperception, including mirror-imagining, warmongering, selling fear, uncritical *technobelief*, and circumstantial factors resulting in the inflation of the concept of war. It concludes that Western political, intelligence, operational, and cyber-technical communities have been overly optimistic and opportunistic in their assessments and predictions on the military utility of cyber operations in war.

The notions of four artistic styles are intended to illustrate the nature of the respective subject matter. Comprehensions of war, a phenomenon and abstraction, are but impressions; projections of capability development remain simplistic, employments of cyber capabilities may be forceful expressions but perhaps partially unrecognisable, and conclusions, or recommendations, are at best point-by-point. The styles are a reminder of the inability of any academic, scientific, or enterprise to fully grasp the nature and manifestations of war.