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.

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.

Part 1. *Impressionism*. On war and cyber warfare

"We shall not enter any publicists' complicated definitions of war, but keep us to the elementary of it, the duel."

Carl von Clausewitz, Vom Kriege (Book 1, Chapter 1:2)

Defining war

War is defined either by its nature or by appearance. Clausewitz, in his remarkably strange trinity, presents the unchanging nature of war as continuously changing around its permanent tendencies.[2] At the same time, he describes war as "not only a political act but a real political instrument"; as "nothing but a widened duel" and as "an act of violence to compel the opponent to do our will."[3]

Quincy Wright, the father of modern war and conflict studies, draws on sociological and philosophical understandings of war to conclude that war is "a socially recognized form of intergroup violence." He notes that war, in the broadest sense, is a violent contact of distinct but similar entities. Most importantly, he recognises that, subjectively, there might be war regardless of seemingly objective legal, political, or sociological definitions of war.[4] Hedley Bull follows Clausewitz when defining war as "organised violence carried by political units against each other." He distinguishes war "in the loose sense of organised violence" waged by political units from "the strict sense of international or interstate war, organised violence waged by sovereign states." Similarly, he distinguishes between war in a materiel sense and war in a legal or normative sense, and he further distinguishes between rational and blind war.[5] Beatrice Heuser, for example, clearly determines situations euphemistically labelled as "emergencies", "troubles", "crisis", and "affairs" as wars: "the use of violence by one organised group against another."[6] Margret MacMillan defines war as organised violence, but notes how different societies fight it differently.[7] Azar Gat, in turn, expands the scope to evolutionary biology, rather than politico-societal affairs and modes of explanation.[8] Mary Kaldor considers that new wars differ from old, modern, and industrialised, wars in terms of their objectives, participants and modes of warfare. In particular, she notes how identity

[2] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999).

[3] Carl von Clausewitz, *Vom Kriege* (Cologne: Ferd. Dümmler Verlag, 1832/1991), Buch 1:1:24, and 1:1:2, respectively.

[4] Quincy Wright, *A Study of War* (Chicago: Chicago University Press, 1942/1966): 5–7.

[5] Hedley Bull, *The Anarchic Society. A Study of Order in World Politics* (New York: Palgrave, 1977/2002): 178–180.

[6] Beatrice Heuser, *The Evolution of Strategy. Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010): 446.

[7] Margaret MacMillan, *War. How Conflict Shaped Us* (London: Profile Books, 2020): 4, 16–17.

[8] Azar Gat, *War in Human Civilization* (Oxford: Oxford University Press, 2006): 1–10.

politics in the 1990s had replaced geopolitical and territorial ambitions, how a plethora of non-state and non-military actors had entered the stage, and how a decentralised global war economy had entirely replaced national and hierarchical modes of production. However, though the primacy of the state in war had diminished, the ”new wars” still appeared to be both highly political and violent.[9]

Warfare, or any other activity-process in wars, campaigns, operations, battles, salvoes, or shots, is but a more concrete expression of a particular manifestation of war. The concept of warfare informs how war can be waged. The chameleon not only changes its colours, but transforms itself as actors, targets, capabilities, and methods and the scale of war oscillate. Understanding war as a phenomenon, rather than a format, extends subsequent political, legal, and moral obligations to inherently violent activities which states, politicians, groups, leaders, and civilian and military operators often wish to downplay and conceal.

War and international law

Christopher Greenwood identifies two schools of thought in how modern international law has approached war. The subjective school has emphasised that it is the intentions of the states concerned which matter. The objective school argues that a situation is to be characterised as war if certain objective criteria are met.[10] Both approaches are untenable; the former because it subjects international law to the lowest or highest bidder, the latter because it is impossible to define and agree on objective criteria. Thus, the problem of analysing an abstraction is replaced by the operationalising of war according to contingent conventions: political, human, and scientific.

For Myres McDougal and Florentino Feliciano, the process of international coercion in its various manifestations, including violence, is a broader and more important issue than war. In particular, they draw attention to the problem of war and peace as striated constructions incapable of reflecting the fluid and complex realities. Referring to Philip Jessup as well as Georg Schwarzenberger, they discuss the need to define an intermediary status, *status mixtus,* in international law. As the name implies, in this site the economic and political power of the state would be supplemented by military power. Such a legal designation would make it more feasible to control coercion and violence in international relations.[11]

Contemporary international law approaches war mainly through its attributes and the appearance of acts of war*.* It is therefore common to speak of, for example, war booty and war prizes, war contributions, war crimes,[12] and, as enshrined in the United Nations Charter, the use of force and armed attack. The latter are considered to create ”thresholds” or “a threshold” “above” of it the International Humanitarian Law, also known as the law of armed conflict, applies.

Bruno Simma notes that the medieval and theological theory of *bellom iustum* never became a valid rule of public international law. Instead, war, “a human feature”, was to be regulated and prevented.[13] While the Covenant of the League of Nations focused on war and

[9] Mary Kaldor, *Nya och gamla krig [New War & Old Wars: Organized Violence in Global Era]* (Göteborg: Daidalos, 1999): 9–17.

[10] Christopher Greenwood, “The Concept of War in Modern International Law”, *The International and Comparative Law Quarterly*, Vol. 36(2) (1987): 283–306.

[11] Myres S. McDougal and Florentino P. Feliciano, *Law and Minimum World Public Order* (New Haven: Yale University Press, 1961): 1–10.

[12] Edmund Jan Osmańczyk, *Encyclopedia of the United Nations and International Agreements*, ed. Anthony Mungo (Abingdon: Routledge, 2003).

[13] Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus, Nikolai Wessendorf (eds.) *The Charter of the United Nations: A Commentary*, Volume II (Oxford: Oxford University Press, 2012): 114–115.

the threat thereof, the United Nations Charter, as noted above, forbids the threat and use of force to save "succeeding generations from the scourge of war."[14] Stephen Neff distinguishes between the main elements of the collective and public character of violence; the fact that it is directed against a foreign state or political entity; the fact that it is a rule-governed, disciplined and rational enterprise; and the existence of rules about the formal commencement of war, which allows for the separation of war from peacetime.[15]

Lassa Oppenheim's definition of war as "a contention between two or more States through their armed forces for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases" highlights another problem: the expectation of a political and military victory.[16] For example, the US justification for not declaring war on North Vietnam referred to the implication of the total destruction of the enemy. It should also be noted that the rather common notions of war and peace having clear legal stages, the Grotian "*inter bellum et pacem nihil est medium*", and the necessity of declarations of war do not correspond to the letter of the law and the practise of contemporary international affairs.[17]

Through the interpretation and application of the UN Charter Article 2(4), war can be considered illegal and, as a legal state, almost extinct. This does not mean, however, that state responsibilities and obligations to other states and the people cease to exist.

International law approximates war. It can only speak of war in terms of legally-defined elements and manifestations of war. Specifically, it considers war to be an inter-national armed, violent conflict[18] in which individual and collective self-defence against armed attack is permitted[19] and in which the UN Security Council may decide, among other measures, to use armed force to give effect to its decisions.[20] International law recognises that war is waged by organised national armed forces, although it recognises the rights of militias, volunteer corps, and organised resistance movements belonging to such Parties to the conflict.[21] It seeks to regulate war by limiting the use, means, and methods of war, such as weapons, weapons systems, ammunition, and harmful substances,[22] and by protecting non-combatants and subsequent property from the harmful, violent effects of war. [23]

Contemporary considerations of how international law treats and should treat the military use of cyber capabilities address the same issues as any state or military use of potentially harmful capabilities. Thus, the applicability of international law, the so called 'existing international law' in cyber affairs, state and non-state actors, the nature and employment of cyber capabilities, the scope and severity of effects, and the appropriate protection of non-combatants and their material and immaterial properties are on the agenda.[24]

[14] League of Nations, *The Covenant of the League of Nations* (1920). United Nations (UN), *Charter of the United Nations* (1945), Preamble.

[15] Stephen C. Neff, *War and the Law of Nations* (Cambridge: Cambridge University Press, 2005): 14.

[16] *Oppenheim's International Law,* 7th edition, vol II, ed. Hersch Lauterpacht (Oxford: Oxford University Press, 1952): 202.

[17] Greenwood, *Concept of War* (see note 10): 284–287, 289–290.

[18] Hague Peace Conference (1899).; UN, *Charter* (see note 14), Articles 2(3), 2(4), 33(1), and 40.

[19] UN, *Charter* (see note 14), Article 51.

[20] Ibid., Articles 41, 42 and 43.

[21] *Convention (III) relative to the Treatment of Prisoners of War* (Geneva, 12 August 1949).

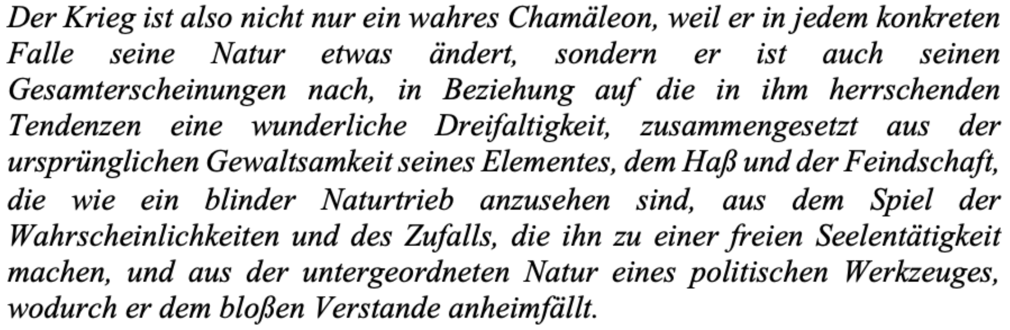
[22] *Hague Convention (IV) respecting the Laws and Customs of War on Land*, (1907); *Protocols I and II additional to the Geneva Conventions* (1977); *Convention on Certain Conventional Weapons (CCW)* (1980) and Amended Protocols (1980, 1996, 2003).

[23] *Convention (IV) relative to the Protection of Civilian Persons in Time of War* (Geneva, 12 August 1949).

[24] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law* 37, (1999): 885–937.; Schmitt (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2027).; Kubo Mačák and Laurent Gisel, "Grammar: Rules in a Cyber Conflict", in *A Language of Power: Cyber*

The Absoluteness of War

The *magnum opus* Marie von Clausewitz edited begins with the final pages her husband wrote, which end with probably the most debated passage of *Vom Kriege*: Book 1, Chapter 1, Paragraph 28; the strange and unpredictable trinity. Here, we are reminded of the elements of violence, hatred, and enmity, described as blind force of nature; the play of probability and chance; and the subordinated nature of a political instrument. A blind passionate and instrumental force which operates imperfectly and unpredictably – how far Clausewitz has come from his initial pursuit of the laws of war! As for seeking solace, many remind the first tendency being attributed more to the people, the second more to the military commander and his army, and the third more to the government.[25]



> *Der Krieg ist also nicht nur ein wahres Chamäleon, weil er in jedem konkreten Falle seine Natur etwas ändert, sondern er ist auch seinen Gesamterscheinungen nach, in Beziehung auf die in ihm herrschenden Tendenzen eine wunderliche Dreifaltigkeit, zusammengesetzt aus der ursprünglichen Gewaltsamkeit seines Elementes, dem Haß und der Feindschaft, die wie ein blinder Naturtrieb anzusehen sind, aus dem Spiel der Wahrscheinlichkeiten und des Zufalls, die ihn zu einer freien Seelentätigkeit machen, und aus der untergeordneten Natur eines politischen Werkzeuges, wodurch er dem bloßen Verstande anheimfällt.*

Because of this famous passage and the very textual reading of it, war has exclusively been seen subjected to the state; no state – no war. This state-centric reading of war has been questioned by a bio-cultural interpretation of war. There, neither the state nor the politics are needed for war to manifest itself: war is embedded in humans and societies, in cultures, and in groins.[26]

But how does that celebrated and contested Book 1, Chapter 1, Paragraph 28 begin? "War is not only like a true chameleon as it, to an extent, changes its nature in each case", but it is also by its total appearance a strange, pulsating phenomenon.[27] War changes beyond recognition, and so does the linguistics, even the grammar, of thinking about it.[28] Dissecting the trinity of hatred, chance and probability, and the subordinate instrumentality helps us to

Defence in the European Union, *Chaillot Paper* no. 176, ed. Patryk Pawlak and François Delerue (2022). Cassese notes that, in the developments of modern armed conflict, new classes of combatants and new agents of destruction have emerged since the Hague Peace Conferences in 1899 and 1907. Whereas the former development refers to such non-state actors as partisans and resistance or liberation movements, Cassese refers to airplanes, submarines, and nuclear weapons as new technologies and armaments initiating reviewing and updating "the traditional rules on warfare." Antonio Cassese, *International Law* (Oxford: Oxford University Press, 2005): 402–404.

[25] von Clausewitz, *Vom Kriege* (see note 3), 1:1:28. Clausewitz regarded the first chapter of the first book the only section as being "completed." Peter Paret considers *Vom Kriege* logical and mainly completed (Peter Paret "Clausewitz.", in *Makers of modern strategy,* ed. Peter Paret (Oxford: Oxford University Press, 1986): 186–213). Paret (p. 201–202) considers the assumptions of people, commander, and government "highly subjective" and of "questionable validity." Cf. Hew Strachan, *Carl von Clausewitz's On War: A Biography* (London: Atlantic Books, 2007).

[26] See, in specific, Martin van Creveld, *The Transformation of War* (New York: Simon & Schuster, 1991).; John Keegan, *The History of Warfare* (London: Hutchinson, 1993).; and Azar Gat, *War in Human Civilization* (Oxford: Oxford University Press, 2006).

[27] von Clausewitz, *Vom Kriege* (see note 3), 1:1:28.

[28] Ibid., 8:2. Here, in a chapter titled "Absolute and Real War", (*Absoluter und wirklicher Krieg*) the ontological difference between war's being (*Wesen*) and its prevailing relations (*Verhältnisse; die gerade vorherrschen*), the play of possibilities, probabilities, good and bad fortune are developed.

move beyond the once-written and later-canonised people-army-government impression of war.

The subordinate, political instrumentality of war provides us with its intention and *raison,* the external context. The trinity itself, its original form and our extended interpretation, does not imply the existence of the state or government. Obviously, the famous line of war being the mere continuation of politics and more, a true political instrument, easily supports an exclusively state-centric interpretation.[29] The culturalists were right to reject the state and government, but for the wrong reasons. Political subordination matters.

A similar instrumental view applies to violence. Violence is not an effect of war, but rather the central means. Accordingly, it is essential to recognise the payloads which signify violence. It has become common to speak of kinetic warfare, especially when distinguishing cyber and information warfare from the more established forms of generating violence in war. Since the notion of "kinetic" obviously refers to the kinetic energy of a moving object, such as a fist, an arrow, or a bullet, it is important to acknowledge the full spectrum of mechanical, thermal, biological, chemical, and radiological effects. The fact that warfare, weapons, and payloads commit violence through energy or toxins situates electronic and electromagnetic payloads and effects within the established conventions of destruction. This condition corresponds to the centrality of destruction in the theory of war.[30] The use of violence can result in anything from a bloody nose to surrender or destroyed data, which is the point. One could argue that, without violence, and linking this to the political subordination thesis, without politically-motivated violence, we cannot speak of war. The concept of violence does not yet entail empirical functionality or efficacy in terms of scale of effect.

Hatred and enmity arise from an awareness of one/another dimension and the necessarily-perceived dispute between two or more entities: the duel. Hatred and enmity help to fuel other more physical forms of violence as means and further justify the (political) use of war. No wonder Clausewitz had earlier noted that war consists of and springs from hostile emotions and hostile intentions. It is no wonder that he noted how wrong it would be to think of war only as an intellectual act of governments.[31] Indeed, Michel Foucault considered that racism makes the relationship of war beyond the military relationship of confrontation "a biological-type relationship."[32]

Chance and probability are similarly inherent and unavoidable conditions of human existence and activity as another one of Clausewitz's famous notions: friction. The play of probability/improbability is not exclusive to war, but it is a typical Clausewitzian observation and warning of how uncertain an enterprise war is: an essentially interactionist affair where the meaning and effect of one's actions depends on the actions/non-actions of others.[33] It is also an example of how the key methodological approach in *Vom Kriege*, the dualism of absolute/ideal and real, functions.[34]

[29] Ibid., 1:1:24.

[30] That is, the notion of familiar structural violence, e.g., from Johan Galtung (Johan Galtung, *Peace by Peaceful Means: Peace and Conflict, Development and Civilization* (London: SAGE, 1996).), is excluded from this discussion.

[31] von Clausewitz, *Vom Kriege* (see note 3), 1:1:3.

[32] Michel Foucault, "Society Must Be Defended", *Lectures at the Collège de France, 1975–1976*, ed. Mauro Bertabi and Alessandro Fontana (New York: Picador 1997): 255–256.

[33] I am in debt to Sebastian Harnisch for this observation.

[34] Clausewitz applied several dualistic equations to portray the richness and complexity of war: politics and war, strategy and tactics, defence and offence, limited and total war, theory and practice, thought and action, art and science; simple and difficult. His method of argument is dualistic rather than dialectic, as both thesis and antithesis prevail: "*dass Krieg ein Ding sein kann, was bald mehr, bald weniger Krieg ist.*" His theoretical considerations were based on using empirical historical examples to explain and illuminate ideas and to support presuppositions and to prove testimonies by deduction. (von Clausewitz, *Vom Kriege* (see note 3), 8:2, and 2:6). See, William F. Owen, "To be Clausewitzian", *Infinity Journal Special Edition* (2012): 20–23; and

Containing a universal quality, a motivational force, and a determining dynamic, the trinity constitutes a core theory of war. Obviously, it does not operate in the manner of a natural scientific theory which explains and accurately predicts outcomes. The power of enlightened science has not been able to penetrate war; the trinity does not offer an ontology of war in which parts, capabilities, and relationships can be used to detect and determine stable and predictable dynamics.

A dictionary definition balances between the Clausewitzian and legalistic understandings of war as "a state of usually open and declared armed hostile conflict between states or nations."[35] Remarkably, the United States Department of Defense *Dictionary of Military and Associated Terms,* otherwise a thorough account, does not define the terms "war" or even "warfare."[36]

War is and remains an absolute abstraction. The absoluteness of war does not give rise to an ontology of war.[37] We can only talk about, understand, and even regulate war only through aspects of war, behaviour in war, reasons for war or a particular episode in time we abstract as war, or some other less-abstract/more-concrete expression. In the process of speaking and analysing war, we move from the abstract of war to a phenomenology of war, from the absolute and complete to the spatial and temporal: the real. It is telling that, determined "to save succeeding generations from the scourge of war", the United Nations Charter prohibits the threat and use of force and mandates individual or collective self-defence if "an armed attack occurs."[38]

This is the way war is being analysed, too, through concrete notions. Antoine-Henri Jomini, another early 19th century military thinker, describes in detail how different types of war should be waged: for example, invasion, intervention, civil and revolutionary, with or without allies.[39]

There is no need to assume that the above-mentioned scholars or lawyers have deliberately wanted to be "Clausewitzian" in emphasising the political instrumentality of states to use violence and destruction against other states or groups. Carl von Clausewitz was simply able to express what war is about. For all his universality, he, too, operated with the linguistic and intellectual concepts and conventions of the time. Therefore, any contemporary, instrumental analysis of his, or anyone else's, thoughts must operate within the dualisms of change and continuity, as well as a textual reading and interpretation.[40]

Hugh Smith, "Clausewitz's Divisions: Analysis by Twos and Threes", *Infinity Journal* Vol 5:3, (2016): 10–13. Cf. Hew Strachan, *Carl von Clausewitz's On War: A Biography* (London: Atlantic Books, 2007).

[35] *Merriam-Webster Online Dictionary*, https://www.merriam-webster.com/dictionary/war (accessed 13 March 2023).

[36] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (2019).

[37] The absoluteness of war does not refer to the notion of absolute war or acknowledge the distorted interpretations of the desirability of an absolute, total war.

[38] UN, *The Charter of the United Nations* (1945), Preamble and Paragraphs 2(4) and 51; Beatrice Heuser, *The Evolution of Strategy. Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010): 444.

[39] Antoine-Henri Jomini, *The Art of War* (London: Greenhill Books, 1838/1992). See also von Clausewitz, *Vom Kriege* (see note 3), 5, 6, 7 and 8:2; and Christopher Daase and James W. Davis (eds.), *Clausewitz on Small War.* (Oxford: Oxford University Press, 1838/1992).

[40] von Clausewitz, *Vom Kriege* (see note 3), 8:2, 8:3b.

Cyber and information warfare

"Cyber war" is an inflated concept, unnecessary and false. For historiographical and populist purposes, we can, if we wish, call a certain episode a cyber war. This would be based on the dominant mode of warfare conducted, a defining characteristic of a war. As noted, this understanding would remain but an impression of war, a fraction of the absolute.

Measured against a Clausewitzian understanding of war, many accounts of cyber war and warfare do not follow methodological or conceptual scrutiny. Some of these accounts, despite their names, do not focus on politically-motivated violent activities against identified groups of people, the hallmarks of war. Instead, they focus on other harmful activities such as crime and hacktivism. For many, "cyber war" is everywhere and constantly raging.[41] It seems particularly popular to talk about cyber weapons.[42] Some denounce the existence of violence in cyber operations.[43] In operational law, a determining question seems to be whether data is an object or not. (In the former case, the protection of the International Humanitarian Law would cover data in the same way as other civilian property.)[44]

In their 1993 account, John Arquilla and David Ronfeldt argue that success in warfare is a function of who has the best information about the battlefield. Accordingly, the information revolution was expected to bring about the next major change in the nature of conflict and warfare. More specifically, they claimed the information revolution would change how societies may come into conflict, as well as how their armed forces may wage war. For Arquilla and Ronfeldt, two new types of warfare seemed likely: netwar and cyberwar. The concept of netwar refers to information-related conflict representing an early thought of what today has become known as information operations, or more bureaucratically, as foreign influence and information interference. Offering a broad spectrum of "wars", the authors explained that "netwar represents a new entry on the spectrum of conflict that spans economic, political, and social as well as military forms of 'war.'" However, they noted that "netwars are not real wars, traditionally defined." Cyberwar, then, they claim, represents military operations according to information-related principles, including the disruption, if not destruction, of the information and communication systems. Cyberwar as a form of warfare was explained as potentially involving various technologies for command, control, communication and intelligence purposes, tactical communications, smart weapon systems, as well as electronic means affecting the information and communications circuits of the enemy: an early prescription of computer network operations. As noted above, Arquilla and Ronfeldt saw cyberwar as signifying a transformation in the nature of war. Given their description of a rather clinical conduct of war at the beginning of the paper, this may be interpreted as a change and reduction of violence in war. In the footsteps of Liddell Hart, the authors raised the Mongols as champions of non-hierarchical warfare.[45]

Half a decade later, Dorothy Denning presented an organised and conceptually more disciplined view on information warfare, indeed a theory of it. Grounding her analysis on the 1991 Gulf War and computerised and "informationised" US military thinking of the 1990s, Denning focused on the value of information resources for offence and defence. Obviously,

[41] See, for example, Charles Arthur, *Cyber Wars. Hacks that shocked the business world* (London: Kogan Page, 2018).; Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly, 2010).; and P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar (*Oxford: Oxford University Press, 2014).

[42] See, for example, Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *The Journal of Strategic Studies* Vol 35:3 (2012): 401–428; David Sanger, *The Perfect Weapon* (2018).; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017).

[43] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Company, 2013).

[44] Schmitt (ed.), *Tallinn Manual 2.0* (see note 24), Chapter 17, section 4.

[45] John Arquilla and David Ronfeldt, *Cyberwar is Coming! Comparative Strategy*, Vol 12:2, (1993): 141–165.

the notion of information warfare is much broader than computers and computer networks. As it is considered to encompass the employment and targeting of all forms and usages of information, it is age-old. However, the speed and penetration of information technologies have given new impetus to information warfare.[46] Denning explained that information warfare consists of offensive and defensive operations which target or exploit information resources. The operational environment is an inherently dualistic and dynamic one: while the offensive "players" seek to increase the availability of information resources and value to themselves, reduce the integrity of the targeted information, and decrease the availability of information recourses and value for the defender, the defensive "players" seek to achieve the opposite: to prevent the availability of their information to any or designated attacker and to ensure the integrity and availability of their information resources. Operations designed to increase or decrease, capture or protect, deny or ensure, or destroy or protect oscillate in an information environment, both offline and online and against digital data, information, and cognitive perceptions. Because the players on either side are individuals, structured or unstructured groups, or state or non-state actors, according to Denning, "anyone can conduct an offensive information warfare operation."[47]

Communist theories of war, military, and insurgency have always viewed war comprehensively. Direct and indirect violence coexist alongside political agitation, which information and disinformation activities seek to take advantage of, creating mutually-reinforcing effects.[48]

Oriental strategic and military thinking in general, Chinese in particular, has been mystified in the West. Ancient Chinese writings are studied because they are thought to reflect fundamentally different approaches to war, strategy, and even politics. Accordingly, contemporary Chinese military thought easily becomes treated as a reflection of its mystified past. But to grant either patronising or glorifying exceptionalism *a priori* is to fail to see a rather similar forest for the partially-different trees.

It is also typical to see Chinese strategic and military theoretical thinking as fundamentally different from Clausewitzian and Western thinking. Lenin, Mao, and Giap clearly recognised the imperative of decisive use of conventional armed force and violence to achieve the political objectives of war, even in the revolutionary wars they fought.[49] Indeed, Mao himself studied Clausewitz during the Great March.[50] He adopted a strategic approach which recognised the utility of political action as well as guerrilla warfare, but emphasised the significance of conventional forces in bringing insurgencies to a victorious conclusion – a view very far from the idealistic interpretation of nonviolent war. A similar approach was

[46] Dorothy E. Denning, *Information Warfare and Security* (Boston: Addison-Wesley, 1999): 10–13.

[47] Ibid: 21–42, see especially Figure 2.1 on page 31.

[48] On Cold War disinformation activities, see Thomas Rid, *Active Measures. The Secret History of Disinformation and Political Warfare* (New York: Farrar, Strauss and Giroux, 2021).

[49] Mao Zedong, "Strategy for the Second Year of the War of Liberation" (1947), Marxist Internet Archive, https://www.marxists.org/reference/archive/mao/selected-works/volume-4/mswv4_21.htm ; Vo Nguyen Giap, *People's War People's Army* (Honolulu: University of Hawaii, 1961) and *How we Won the War* (Philadelphia: Recon Publications, 1976); George K. Tanham, *Communist Revolutionary Warfare: From the Vietminh to the Viet Cong* (Westport: Praeger, 2006/1961).; Mika Kerttunen, "A transformed insurgency: The strategy of the Communist Party of Nepal (Maoist) in the light of communist insurgency theories and a modified Beaufrean exterior/interior framework", *Small Wars & Insurgencies*, Vol 22:01 (2011): 78–118. Giap's impatience and the role conventional forces had in Vietnamese thinking, as well as in the battlefield, contradicts Keegan's notion of Oriental warfare being "something different and apart from European warfare" and characterised by the peculiar traits of "evasion, delay and indirectness" (Keegan, *History of Warfare* (see note 26): 387).

[50] Owen, "To be Clausewitzian" (see note 34); Matti Nojonen, "Classical and some contemporary Chinese views on strategy", Conference presentation, *Cyber Strategy Formulation and Leadership* (Baltic Defence College, Tartu: 21 February 2013).

adopted by Hanoi in the Vietnam War between 1955 and 1975.[51] Guerrilla warfare, terrorism, and political-informational fronts were considered useful to engage and wear down the enemy, to raise awareness, and to gather sympathy even within the ranks of the enemy, but not sufficient to resolve (the) war.

Obviously, the nature and particular characteristics of war, strategy and politics are contingent and constantly shifting, but their tendencies are universal; the human being with her cognition is the same and technology and the laws of nature are the same.[52] Therefore, Chinese views on information war and warfare are interpreted here as similar to, rather than different from, the Occidental ones. The development of Chinese informational approaches to war and capabilities for network operations is obviously a story of transformation.

Lyu Jinghua locates the beginning of the China's academic discussion of cyber warfare in the 1990s when the US military activities in the first Gulf War (1990-91) and Kosovo (1999) demonstrated the enabling effect of digitalised information. Similarly, the rapid defeat of Saddam Hussein's industrialised (and Soviet-era) army in 2004, prompted the People's Liberation Army to introduce the concept of "informationisation" in its 2004 white paper.[53] Gurmeet Kanwal also identified the 1997 Chinese thought of "acupuncture warfare", or the practice of paralysing the (conventionally superior) enemy by attacking the weak points of his command and communication and information systems.[54]

Also drawing from the 1991 Gulf War, Liang and Xiangsui argue that war and modes of war have changed and expanded to include non-lethal and non-military spheres, types of operation, and means of engagement "to compel the enemy to accept one's interests." Recalling that warfare is a "dynamic process full of randomness and creativity", they remain sceptical that any one technology alone would help to win future wars. Their warning that any attempt to bind war to a set of ideas within a predetermined plan is little short of absurdity or naiveté testifies to real wars and the Clausewitzian concept of war.[55]

Lyu Jinghua notes a theoretical debate in China about whether it is wiser to invest in cyber defence or offence. Although cyberspace is portrayed as offence-dominated, the advocates of strong defence emphasise the need to survive an offensive in order to respond. [56] Juha Vuori observes that the concept of deterrence is missing from the Chinese cyber affairs discourse. He explains the absence by Chinese (or any state's) vulnerability to cyberattacks: deterrence by denial is not credible and deterrence by punishment is counterproductive.[57] China has consistently resisted references to International Humanitarian Law in the UN Group of Governmental Expert negotiations, seeing this as a tacit acknowledgement

[51] Vo Nguyen Giap, *People's War People's Army*. (Honolulu: University of Hawaii, 1961).

[52] See Gray for the argument of the universality of strategic thinking (Colin S. Gray "Strategic culture as context. The first generation of theory strikes back" (1999), republished in Colin S. Gray, *Strategy and History. Essays on theory and practice* (Abingdon: Routledge, 2006): 151–169).

[53] Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?", *IPI Global Observatory*, 22 March 2019, https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/ (accessed 13 March 2023).

[54] Gurmeet Kanwal, "China's Emerging Cyber War Doctrine", *Journal of Defence Studies*, Vol. 3:3 (2009), https://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf (accessed 13 March 2023).

[55] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Panama City: Pan American Publishing House, 2002): xix–xxii, 7–10, 185.

[56] Lyu Jinghua, *China's Cyber Capabilities* (see note 53). Cf. Timothy L. Thomas, *Three Faces of the Cyber Dragon* (Ft. Leavenworth: Foreign Military Studies Office, 2012): 150–151. Whether offence or defence is stronger, or in modern terms: more resilient, see von Clausewitz, *Vom Kriege* (see note 3), 6:1–7, as well as James Farwell and Rafal Rohozinski, "The New Reality of Cyber War", *Survival* 54:4, (2012): 107–120.

[57] Juha Vuori, "The Curious Absence of Chinese Cyber Deterrence", *Directions. Cyber Digital Europe,* 2022, https://directionsblog.eu/the-curious-absence-of-chinese-cyber-deterrence/ (accessed 13 March 2023).

of the militarisation of cyberspace and an implicit legitimisation of the employment of military cyber capabilities in war.[58]

Nearly a decade ago, Amy Chang noted that Chinese military cyberspace efforts focussed on preparing for military scenarios and ensuring military superiority in the event of cybered conflict with an adversary through military modernisation, computer network operations research, and human capital cultivation.[59] Indeed, the PLA dictionary explains of information offence (*xinxi jingong*) as "information attacks" in which information warfare technology is utilised to interfere and sabotage enemy information operations and information systems, and in which both electronic and network attacks are employed. Moreover, the purpose is, in the manner of Western cyberspace and information operations, to affect and weaken the enemy's information acquisition, transmission, processing, and utilisation decisions.[60] Referring to a 2013 publication, Chang identifies the types of military conflict in the network domain as network reconnaissance, network attack and defence operations, and network deterrence, as well as ways to prepare for potential military conflict in the network domain.[61]

Martin Libicki draws a distinction between strategic cyberwar and operational cyberwar. While the former consists of "a campaign of cyberattacks launched by one entity against a state and its society" with the purpose of affecting the target state's behaviour, the latter employs computer network attacks "to support physical military operations." In short, in a strategic cyberwar, no other active hostilities are taking place. In fact, mutual confidence between two states that strategic cyberwar will not lead to a physical conflict will enable and encourage conducting it. Like any other type of war, Libicki argues, cyberwar can begin with deliberate provocation and escalation. In terms of the objectives of war, cyberwar cannot disarm, "much less destroy", the enemy. Moreover, in the absence of physical combat and violence, cyberwar cannot lead to any territorial gains.[62]

Libicki goes on to describe how (strategic) cyberwar would be waged. Because there are many options to consider, cyberwar may initially appear to be incremental. This perception may prove to be false. The unpredictable and nonlinear relationship between the efforts and effects of cyber operations may unintentionally escalate the situation. All in all, the strategic and operational considerations operate in an interplay in which the existence/non-existence of other forms of hostilities condition the nature of cyberwar, too. Libicki considers a *sub rosa*, hidden cyberwar plausible.[63]

Operational cyberwar or wartime cyberattacks against military or justifiable civilian targets is less concerned with escalation; a war or a violent, armed attack is already taking place. Libicki screened out computer network exploitation (espionage), electronic interference, and psychological operations, as well as physical attacks on networks or information and communication systems. Cyber-digital effects are to be created in cyber-digital systems by cyber-digital means. However, even operational cyberwar cannot win "an overall war on its own." Operational cyberwar, Libicki concluded, could quickly cripple adversary

[58] Own observations from the UN GGE negotiations and UNIDIR and regional cyber security conferences in 2014–2019.

[59] Amy Chang, *Warring State China's Cybersecurity Strategy* (Center for a New American Security, 2014): 8, 14, https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142&focal=none (accessed 13 March 2023).

[60] PLA Military Technology Management Committee. *Military Terminology.* Translated by Amy Chang. Referred in Chang, *China's Cybersecurity Strategy* (see note 59): 14.

[61] Chang, *China's Cybersecurity Strategy* (see note 59): 25.

[62] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: Rand, 2009): 117–122.

[63] Ibid: 125–126, 128–129.

capabilities, provide a temporary (but potentially decisive) advantage, and prevent the adversary from using its systems in confidence.[64]

Departing from Clausewitz, Thomas Rid emphasises that, absent of violence, cyber-attacks cannot be regarded acts of war. "A real act of war", he claims, is always potentially lethal. In examining violence, Rid observes how code-caused violence is indirect; that code does not have (violent) force or energy of its own. He does not deny code-induced violence, but considers it "physically, emotionally and symbolically limited." He also is sceptical about whether cyber-attacks can be considered instrumental or political, either.[65]

Rid recognises three forms of cyber offences: subversion, espionage, and sabotage. Because of its technical nature, sabotage does not count as violence proper, according to him. Stating that "*things are the prime targets, not humans*" (original emphasis), he underlines the human body as the original source and ultimate recipient of violent force. Rid considers affirmative evidence of the war-like nature of cyber-attacks insufficient. For example, he acknowledges that attacks on industrial control systems are "the most probable way for a computer attack to create physical damage and indirectly injure or kill people."[66]

Alongside with Rid's argumentation, Ben Buchanan criticises the overextended discussion of cyberwar. He recalls that the employment of cyber capabilities produces less harm than conventional/proper military means, for example, by target specificity, which limits usability and instrumentality. Buchanan points out that cyber capabilities alone cannot deter and resolve matters of war. He concludes that conflict, rather than war, might be a more useful framework for understanding the peacetime employment of scalable, potent, and contingently-instrumental cyber capabilities.[67]

Richard Clarke and Robert Knake warn that cyber war could increase the likelihood of "a more traditional combat with explosives, bullets, and missiles", and could even make a conventional attack easier. They cite the 2003 US-Iraq War and the 2007 Israeli Operation Orchard as examples. Another tried-and-tested way of waging cyber war is to send propaganda to demoralise the enemy. They also distinguish stand-alone cyber war, in which effect-creating cyber capabilities would be used outside of an armed conflict, from war proper. The distributed denial-of-service attacks against Estonia in spring 2007 were cited as examples of politically-motivated employments of malicious cyber means. Clarke and Knake conclude that cyber war is real, global, moving at the speed of light, bypassing the battlefield, and has already begun. In the future, they claim, "most kinetic wars will be accompanied by cyber war" and "other cyber wars will be conducted as 'stand-alone' activities."[68]

Frans Osinga warns against the unclear transition from cyber-attacks to political objectives as "war is political", while cyber-attacks are mainly criminal by nature and indirect in effects. In the same vein, he points out that the level of uncertainty about effects and measures of success is much higher than in so-called kinetic attacks.[69]

Chris Demchak, in turn, contextualises cybered conflict in terms of the fundamental need of nation-states to gain access to accurate and up-to-date data, even if done so in an aggressive manner. This was done to ensure the overwhelming foreknowledge needed to control

[64] Libicki, *Cyberdeterrence* (see note 62): 139–142.

[65] Rid, *Cyber War* (see note 43): 1–2, 11–21, 34.

[66] Ibid: 56–61.

[67] Ben Buchanan, "Cyberwar Redux", in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford: Oxford University Press, 2020): 239–250. See also Kello on how "the virtual weapon" allows new forms of strategic effects which do not involve violence (Kello, *Virtual Weapon* [see note 42]: 196).

[68] Richard A. Clarke and Robert K. Knake, *Cyber War, The Next Threat to National Security and What to Do about it* (New York: HarperCollins, 2010): xiii, 10–16, 30–32.

[69] Frans Osinga "Introducing Cyber Warfare", in *Cyber Warfare. Critical Perspectives*, ed. Paul Duchaine, Frans Osinga and Joseph Soeters (The Hague: T.M.C. Asser Press, 2012).

the outcomes of a nation's complex socio-technical-economic systems. For her, cybered conflict proceeds beyond the mere military tactical salvos or hacking schemes to a broad system-versus-system struggle; one could claim the Clausewitzian idea of duel is therefore taking place at every level.[70]

Echoing Arquilla and Ronfeldt's elaborations on netwar and cyberwar, Max Smeets suggests that offensive cyber capabilities can be used effectively with few casualties and achieve a kind of psychological ascendancy. Since the notion of strategic value was seen as supporting deterrence and producing a conflict or battlefield outcome, we can assume that the question is about the effect-creating quality of offensive capabilities, that of violence against data and information systems. Offensive cyber operations were seen as computer activities to disrupt, deny, degrade, or destroy – a menu which became public in the revealed 2012 Presidential Policy Directive PPD-20, "U.S. Cyber Operations Policy", signed by President Obama. Smeets notes that "an offensive cyber operation should not be considered by itself but with reference to both its direct and indirect effect upon conflict." Most importantly, Smeets recognises that offensive cyber operations have value and are conducted regardless of a formal or *de facto* state of war. The recognition that the deployment of offensive cyber capabilities may (or may not) escalate a situation falls short of acknowledging that offensive cyber operations constitute war.[71]

Referring to an Organization of Economic Cooperation and Development (OECD) definition, Matthew Ford and Andrew Hoskins view war as a form of political violence involving "the use of force to achieve a political end that is perpetrated to advance the position of a person or a group defined their position in society."[72] They note how data and (smart and) connected devices have proliferated and altered ways of political, societal, and military operational behaviour, including war. In the process, they claim, Clausewitz's trinity of state, people, and armed forces has become irrelevant. In this process of widened participation and increased speed, war and its representation have merged. It is as if wars have no end or beginning.

If everything is used and can be used for the purposes of war, or every act can be considered as warlike, what is left is a constant state of *warre*, political nihilism, and increased openings for securitisation and militarisation of life, liberal democratic life, and peace. Writing on strategic theory, Raoul Castex observes the transformation of space and time (in naval warfare), that the enemy (equipped with submarines and airplanes) can be expected to appear anywhere and at any time, that the "combat has been extended in time, as well as in space"; indeed, that the period of complete rest is but a distant memory.[73]

[70] Chris Demchak, "Cybered conflict, hybrid war, and informatization wars", in *Routledge Handbook of International Cybersecurity*, ed. Mika Kerttunen and Eneken Tikk (Abingdon: Routledge, 2020): 36–51.

[71] Max Smeets, "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly* (2018): 90–113.

[72] Matthew Ford and Andrew Hoskins, *Radical War. Data, attention and control in the 21st century* (London: Hurst & Company, 2022): xv–xix, 6–7, 10, 47–56, 195–201, 203. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare.* (Panama City: Pan American Publishing House, 2002): xix–xxii.

[73] Raoul Castex, *Strategic Theories,* ed. Eugenia C. Kiesling (Annapolis: Naval Institute Press, 1994): 14–15.

Part 2. *Naturalism.* Military cyber doctrines and units

"But there is another way. It is possible to increase the likelihood of success without defeating the enemy's forces."

Carl von Clausewitz, Vom Kriege (Book 1, Chapter 2)

The history of how computers have been utilised in and for military operations testifies to the ideals behind cyber operations. As early as the Second World War, computers were used to calculate trajectories and mathematical models for weapons development and operational analysis. In the early years of the Cold War, computing was increasingly used to combine the observations from air defence and early warning stations both in North America and the Soviet Union. This required the establishment of lines and means of communication between computers and their stations. The advent of packet-switching technology in the late 1950s expanded the possibilities for communication and connectivity. A further leap in capacity emerged in mid-1960s with the programmable IBM mainframe. The digitalisation of the battlefield began in earnest in the 1980s with precision weapons with more accurate targeting sensors. The proliferation of computers and other digitalised technologies gave impetus to the concept of a Revolution in Military Affairs, perhaps best characterised by the combination of new technologies, innovative operational concepts, and changing the nature of conflict. The collapse of the Soviet Union created opportunities for both faster and lighter expeditionary operations, while leaner force structures also arose in the West. The Gulf War in 1990–1991 and the Kosovo War in 1999 demonstrated the power of an informationised operational environment. The operational concepts of manoeuvre warfare, centre of gravity, and of a network-centric approach emphasised surprise, paralysing precision effects, and seamless jointness of action. In the new millennium, technologies such as radiophony, telephony, computing, and optical and artificial sensors have merged, epitomised in the notion of "smart." Similarly, the previously separate domains of intelligence, manoeuvre operations and network operations, and electronic warfare began to merge and blur.[74]

[74] Eneken Tikk-Ringas (ed.), *Evolution of the Cyber Domain: The Implications for National and Global Security* (London: International Institute for Strategic Studies/Routledge, 2015), https://www.iiss.org/publications/strategic-dossiers/evolution-of-the-cyber-domain (accessed 13 March 2023).

Better means, better effects

Military cyber capabilities are believed to provide states with better ways to project power and create harmful effects on adversary targets. "Cyber", primarily computer network operations, are commonly seen as fast, cheap, stealthy, and effective. While this understanding can be challenged, military cyber capabilities are seen as potent and valuable to national state prowess.

A 2013 United Nations Institute for Disarmament Research report, which surveyed 193 states, found that "32 states included cyberwarfare in their military planning and organisations, while 36 states had civilian agencies charged with a domestic cybersecurity mission." The report also stated that the number of national cybersecurity programmes had risen to 114.[75] Many analysts and diplomats concerned about the militarisation of cyberspace were quick to refer to the report.[76] However, a closer reading of the report reveals that of the 193 countries assessed, 114 had national cybersecurity programmes, 67 of which had only civilian programmes. Moreover, 41 countries were found to have some sort of military cyber programme, of which 27 had established military cyber units and seventeen were developing offensive military cyber capabilities. In fact, only six states were noted to have published military cyber strategies (with varying degrees of detail and specificity).[77]

It was reported in January 2017 that the United States intelligence community estimated that there were "30 countries building cyber-attack capabilities", or alternatively, "more than 30 states were developing offensive cyber capabilities."[78] In fact, what was said was that "collectively there are 30 nations right now that have some level of cyber capability. There are four or five of them that are near peer to the United States." But it was not the US intelligence officials (James Clapper, Marcel Lettre, and Michael Rogers) who uttered the numbers, but Senator Thomas Tillis. The estimated number presented before the U.S. Senate Armed Services Committee emphasised Russian hacking, election interference, information operations, and cyber espionage capabilities, but made no mention of Russian military cyber capabilities.[79]

Jason Blessing has perhaps most accurately enumerated the "cyber forces", or the "active-duty military organizations with the capability and authority to direct and control strategic cyberspace operations to influence strategic diplomatic and/or military interactions", that countries have developed. By 2018, sixty-one countries had some form of a military cyber force. Blessing's analysis did not differentiate as to whether all nations had offensive capabilities or whether they had focussed on situational awareness, defence, and information operations. At the observed average rate of four to five new countries "joining the club", in 2023 the number could be closer to eighty.[80] However, as with the issuing of

[75] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities" (Geneva: UNIDIR, 2013): 1.

[76] Personal observation from several UN, UNIDIR, EU cyber diplomacy and cybersecurity conferences.

[77] UNIDIR, "Cyber Index" (see note 75): 2–5.

[78] "US intelligence: 30 countries building cyber-attack capabilities", *ZDNET,* 5 January 2017, https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/ (accessed 13 March 2023) and Tom Uren, Bart Hogeveen and Fergus Hanson, "Defining offensive cyber capabilities" (Australian Strategic Policy Institute, 2017), respectively.

[79] James R. Clapper, Marcel J. Lettre II and Michael S. Rogers, "Foreign Cyber Threats to the United States", Testimony before the U.S. Senate Arms Services Committee, 5 January 2017, https://www.armed-services.senate.gov/imo/media/doc/17-01_01-05-17.pdf (accessed 13 March 2023).

[80] Jakob Blessing, "The Global Spread of Cyber Forces, 2000–2018", in *Going Viral,* ed. T. Jančárková, L. Lindström, and P. Zotz (Tallinn: CCDCOE, 2021): 233–255.

national cyber or information security strategies or doctrines, a saturation point may already have been reached.[81]

Even in the development of military cyber capabilities, the reality is less than absolute. States developing cybersecurity have focussed on fundamental capacities and capabilities such as legislation, strategies, governance systems and organisations, combatting cybercrime, protecting critical infrastructure, workforce development, and public awareness. At the same time, armed and defence forces have struggled to computerise and digitalise their non-operational and operational activities. This work has ranged from network deployment, network monitoring, and enhancement of basic cybersecurity capacities to the development of military cyber units and respective war-fighting capabilities. Few countries have deployable, employable, and sustainable military cyber capabilities. "Script kiddies", hacker groups, and patriotic volunteerism do not constitute sustainable military forces.[82]

In order to determine the extent of cyber-digital employment in battles and war, we can define a heuristic model ranging from no cyber-digital to only cyber-digital employment (see Table 1 below). While it may be possible to conduct a battle or operation without any digital impact or footprint, any major military campaign or war will involve some use of digital devices, services, and data. Finally, while it may be possible to conduct fully cyber-digital engagements and operations, it is unlikely that cyber-digital means and methods would completely replace the conventional ways of warfare, but rather, they will support them.[83]

Military activity	**No cyber-digital usage**	**Cyber-digital support**	**Only cyber-digital usage**
War	Not likely	Joint functions, tactical usage of weapons systems and platforms	Not applicable
Campaign	Unlikely		Unlikely
Operation	Brute violence		Computer network operations including signal intelligence and electronic warfare
Engagement			

Table 1. The use of cyber-digital means at various levels of violent military activities.
Developed from: Mika Kerttunen, "Cyber War from Science Fiction to Reality", *Sicherheit und Frieden*, 36:1 (2018): 27-33, DOI: 10.5771/0175-274X-2018-1-27.

[81] For national cyber or information security strategies, see Eneken Tikk and Mika Kerttunen, *Strategically normative. Norms and principles in national cybersecurity strategies* (Brussels, EU ISS, 2019), https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/w7_Wb09c/kerttunen_tikk-strategically-normative-april-2019-eucyberdirect_.pdf (accessed 13 March 2023), and *Annex to* "Strategically normative. Norms and principles in national cybersecurity strategies" (Brussels, EU ISS, 2019), https://eucyberdirect.eu/content_research/1230/ (accessed 13 March 2023). Unfortunately, most of the portals lack behind the latest versions (e.g., Australia and the US issuing their latest strategies in February and March 2023, respectively) and they do not include the earlier versions of similar national guiding documents.

[82] Mika Kerttunen and Eneken Tikk, *Strategically normative. Norms and principles in national cybersecurity strategies,* EU Cyber Direct (2019).; Mika Kerttunen, "The Role of Defence in National Cyber Security", in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford: Oxford University Press, 2021), and Max Smeets, *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022).

[83] Mika Kerttunen, "Cyber War from Science Fiction to Reality", *Sicherheit und Frieden*, 36:1 (2018): 27–33, DOI: 10.5771/0175-274X-2018-1-27.

This analysis manifests the dualism between online and offline (or: virtual-digital and physical) military activities. It is unlikely that there will be only one type of activity in any major engagement; on the contrary, online and offline activities will interact with varying intensity and relevance.

Similarly, Matthias Schulze has identified a continuum of expected cyber activity prior to the Russo-Ukrainian War. As shown in Figure 1 below, his model is organised according to the expected effect. Here, information operations with potential cognitive effects do not directly affect technical systems and services. At the other end of the continuum, "Cyber Pearl Harbor" indicates large-scale physical destruction.[84]

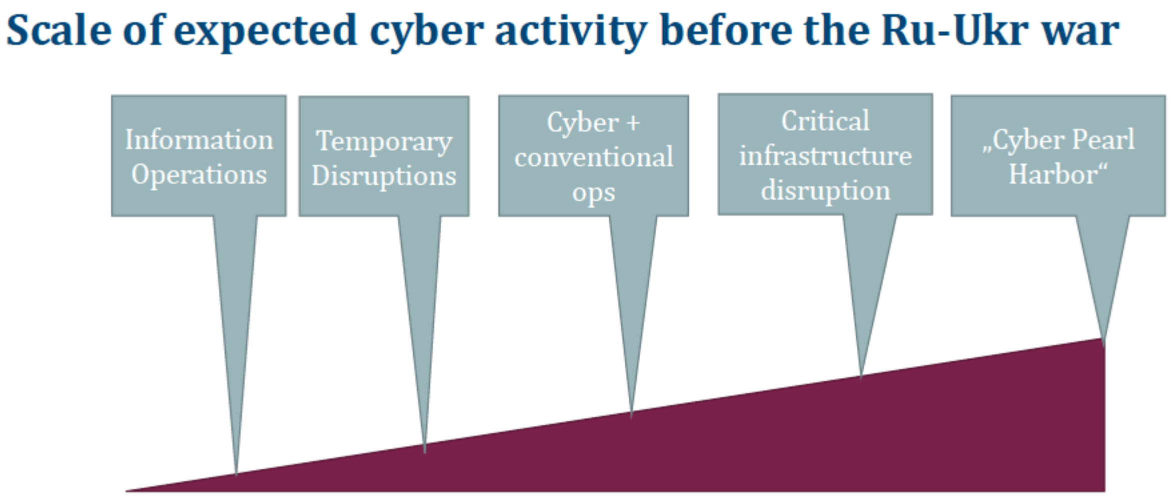

Scale of expected cyber activity before the Ru-Ukr war
Information Operations
Temporary Disruptions
Cyber + conventional ops
Critical infrastructure disruption
„Cyber Pearl Harbor"

Figure 1. The Scale of expected cyber activity before the Russo-Ukrainian War. Source: Matthias Schulze, "Early lessons from the cyber and digital dimension of the Russo-Ukrainian war", Presentation, Stiftung Wissenschaft und Politik (2022).

In designing doctrinal, organisational, technical, and educational answers to the puzzle of the utility and employment of military cyber capabilities in war, some states have declared cyberspace a new domain of warfare.[85] It is too early to determine whether such a declaration will bring benefits other than an organisational identity with exclusive responsibilities. Conceptually, such a move, if implemented, may enhance effectiveness within its realm. It may also further isolate and alienate cyberspace operations from the established armed services. Coupled with an increased appetite for domestic and peacetime operations, the existence of cyber domain *specialis* may expand the space *vulgaris* of the executive and reduce political accountability.[86]

[84] Matthias Schulze, "Early lessons from the cyber and digital dimension of the Russo-Ukrainian war", Presentation, Stiftung Wissenschaft und Politik (2022). One should note that Pearl Harbor perhaps more signifies a tactical surprise than a so-called decisive battle; moreover, although causing vast destruction at the harbour, the strategic impact of "Pearl Harbor" was counterproductive for Japanese and Axis war efforts.

[85] See, for example, NATO, "NATO Cyber Defence", August 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf (accessed 13 March 2023), and NATO CCDCOE, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit", 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ (accessed 13 March 2023).

[86] The European Repository of Cyber Incidents (EuRepoC; https://eurepoc.eu/) continues to pay attention to the development and deployment of military cyber capabilities through analysis of national Military Cyber Units (MCU), Advanced Persistent Threat (APT) actors, Major Cyber Incidents (MaCI), and legal, political, and technical analysis of civilian and military cyber power projection and other affairs.

Military cyber doctrines and units: liberal and authoritarian schools of thought

Military cyber doctrines

Similar to other military breakthrough technologies such as machine guns, aircraft, and nuclear weapons, the operational employment of digital information and communication technologies can be seen as a path of technological and conceptual innovation, integration of operations and effects, and normalisation of activities. Without drawing clear boundaries, the operational, battlefield use of military cyber capabilities may (still) remain between innovation and integration.[87]

The example of the US military cyber capabilities, including doctrines and units, is presented here as a benchmark against which decisions and developments elsewhere in the industrialised West and beyond can be contrasted or compared.[88] As noted above, the Other is represented by an authoritarian model of governance, violence, and operations. This is perhaps best epitomised by the Russian and Chinese way of organising military cyber power.

Building on the 1990s command and control warfare, information warfare, and information operations doctrines of the 1990s and the operational practice of the 1990–1991 Gulf War, Kosovo in 1999, and Operation Iraqi Freedom and Operation Enduring Freedom, the 2006 *The National Military Strategy for Cyberspace Operations* (NMS-CO) described the cyberspace domain and provided a strategic framework for action for "using cyberspace operations to assure US military strategic superiority in the domain."[89] The NMS-CO outlined operational parameters for the Department of Defense (DOD) main mission of defending the nation. The DOD was directed "to execute the full range of military operations in and through cyberspace to defeat, dissuade, and deter threats against U.S. interests." In addition, the DOD was to "use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive options." [90] In sum, computer network attacks were to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[91]

[87] See, e.g., Tikk-Ringas (ed.), *Cyber Domain* (see note 74).

[88] This methodological choice does not subscribe to the United States' intellectual, normative, or doctrinal superiority but to its comprehensiveness and transparency.

[89] Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations (NMS-CO),* Declassified edition, Memorandum (2006).

[90] Ibid: 2. In the missions of "national incident response" and "critical infrastructure protection", DOD was to offer support to civilian authorities, the Department of Homeland Defense, and other federal departments and agencies.

[91] Ibid, Glossary. Later, the 2012 Presidential Policy Directive PPD-20 *U.S. Cyber Operations Policy* authorised the ontology of cyber effects as "[T]he manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon." It should be noted that the PPD-20 does not differentiate which authority or agency conducts cyber operations; "nothing" in the directive was intended to alter the existing authorities of, or grant new authorities to, any U.S. Government department or agency. (The White House, *U.S. Cyber Operations Policy,* Presidential Policy Directive PPD-20 (2012)). The PPD-20 was leaked and formally remains top secret and regarded as a stolen document. It was first published in *The Guardian* and later in many US websites.

Cyberspace operations to gain and maintain the initiative, a classic military theoretical value, and to deter adversaries from "establishing or employing offensive capabilities against US interests in cyberspace" required the DOD to be able to operate within adversary decision cycles and integrate cyberspace capabilities across the full range of military operations. To underscore the joint and similar nature of military cyberspace operations, the NMS-CO outlined, among other things, the development of "processes for cyberspace targeting, collateral damage estimation, standing and special Rules of Engagement, and measures of effectiveness assessments that are integrated within the joint force targeting process and result in tailored, effects-based operations that support joint commander objectives, guidance, and intent."[92]

The current US joint cyberspace doctrine (JP 3-12) views cyberspace capabilities as providing and sustaining "continuing advantages in the operational environment and enable the nation's economic and physical security." The joint doctrine recalls that while cyberspace operations can "produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate most cyberspace operations with other operations to create coordinated and synchronized effects required to support mission accomplishment." Indeed, due to the complexity of cyberspace, it is not considered possible to maintain global or even local cyberspace superiority in perpetuity; this technological and operational deficit requires commanders to "be prepared to conduct operations under degraded conditions in cyberspace."[93]

Cyberspace operations are categorised as offensive, defensive, or DOD information network support missions based on the intent or objective of the issuing authority, regardless of the cyberspace actions conducted, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities employed.

[92] *NMS-CO* (see note 89): 13 and Enclosure F. Enclosure F explicitly ties the process of integration to the *DOTMLPF* framework of military capability development (see the next section on the development of military cyber units).

[93] Joint Chiefs of Staff, *Cyberspace Operations, JP 3-12* (8 June 2018): I-1 – II-2.

The following illustration demonstrates the operational complexity of cyberspace.

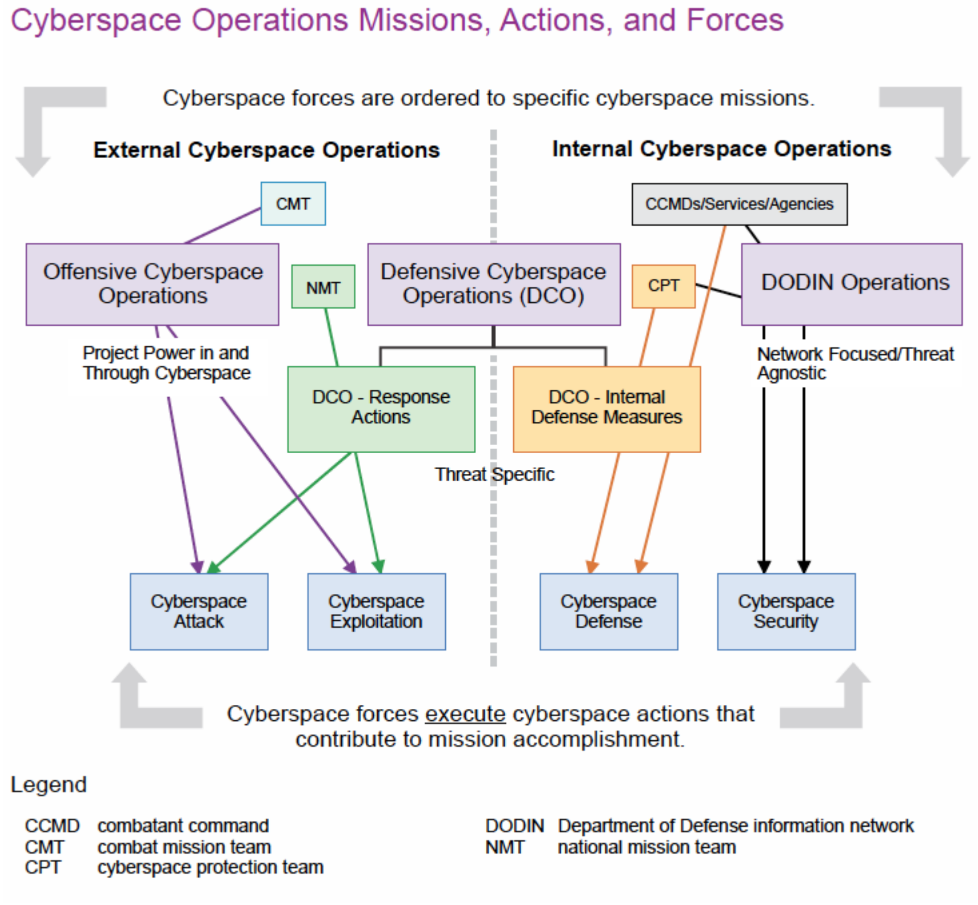

Cyberspace Operations Missions, Actions, and Forces
Cyberspace forces are ordered to specific cyberspace missions.
External Cyberspace Operations
Internal Cyberspace Operations
CMT
CCMDs/Services/Agencies
Offensive Cyberspace Operations
NMT
Defensive Cyberspace Operations (DCO)
CPT
DODIN Operations
Project Power in and Through Cyberspace
Network Focused/Threat Agnostic
DCO - Response Actions
DCO - Internal Defense Measures
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.
Legend
CCMD combatant command
CMT combat mission team
CPT cyberspace protection team
DODIN Department of Defense information network
NMT national mission team

Figure 2. The US Department of Defense Cyberspace Missions, Actions, and Forces.
Source: Joint Chiefs of Staff, *Cyberspace Operations, JP 3-12* (8 June 2018), p. II-3.

To understand the employment of cyber capabilities in war, the category of cyberspace attack provides the most added value, as defending or sustaining networks is takes place predominately during peacetime and probably includes less violent activities. Accordingly, cyberspace attacks are carried out to create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace, or manipulation, leading to denial effects in the physical domains. This is an important distinction from both cyberspace exploitation actions, i.e., intelligence activities, and information operations. To emphasise the difference between cyberspace exploitation actions intended to remain clandestine, i.e., network intelligence activities, and information operations, which directly target and influence human cognition, perception, and behaviour, it is said that cyberspace attack actions become "apparent to system operators or users, either immediately or eventually, since they remove some user functionality." Moreover, cyberspace attack actions to prevent access to, operation of, or availability of a target function (denial) or actions that control or change information, information systems, and/or networks to create physical denial effects are considered a form of fires. These activities are to be coordinated with other departments and agencies, and "carefully synchronized with planned fires in the physical domains."[94]

[94] Ibid: II–7.

And herein lies the core Western thought of employment of military cyber capabilities in war: they are capable of creating noticeable effects; temporary or permanent; reversible or irreversible; hostile to the targeted entity; and violent to the targeted devices, systems, or information in direct or indirect conjunction with other types of military activity. The fact that cyber-digital assets support other types of military fires and activities does not make them cyber operations; similarly, that cyber-digital assets are also employed by civilian, law enforcement or national intelligence agencies does not make that employment military. That military cyber capabilities may be employed outside of factual or legal boundaries of war and may or may not constitute an act of war, that governments project their violent power through cyberspace even in peacetime, or that the notions of cyber war and cyberwarfare are used to explain a wide range of harmful cyber activities do not undermine, but rather underscore the importance of understanding the employment of military cyber capabilities in war. Even if the terms of military cyber operations or military cyber units are irrelevant or unhelpful, this does not dilute the question of how armed forces are employing cyber capabilities in war.[95]

Indeed, by listing signals intelligence, network defence, traditional electronic warfare, influence campaigns, military deception, and military information support operations among activities where existing authorities were not to be pertained or altered, *PPD-20* acknowledges the cross-domain relationships and operational potential of cyberspace activities, whether intended or not.[96]

The American model, first and perhaps best embodied in the 2006 *National Military Strategy for Cyberspace Operations,* constructed the wheel that many wealthy nations want to possess and contemporary authors are trying to reinvent. But there is another way of integrating and operating with military cyber activities: the Russian security and intelligence apparatus-driven subversive and oppressive one.

In Russia, the interconnectedness of actions is a doctrinal virtue. The Kremlin uses the notions of "information security" and "information warfare" in an encompassing manner and, in the Soviet tradition, to align all state activities to secure the state from any form of adversary influence, mainly that of the US and the West. As the 2000/2008 Russian information security doctrine declares, "[B]y the information security of the Russian Federation is meant the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state."[97]

When discussing Russian cyber operations, attention is often rightly focussed on either various malware attacks or network exploitation ("cyber espionage") against civilian targets or political processes. Similarly, reports highlight the involvement of the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), the Main Directorate General Staff (GRU), and non-state actor groups, usually labelled in the West as APTs, short for Advanced Persistent Threats. It is also typical to speak of information or influence operations using or exploiting cyber-digital systems and services, including social media platforms.[98] For

[95] Eneken Tikk, "The Intelligence Function and World Order", in *Research Handbook on Intelligence and International Law*, ed. Inaki Navarrete and Russel Buchan (London: Edward Elgar, forthcoming 2023).

[96] *PPD-20* (see note 91): 5–6.

[97] The Kremlin, *Information Security Doctrine of the Russian Federation* (2000/2008).

[98] See, for example, Ben Buchanan and Michael Sulmeyer, "Russia and Cyber Operations", Carnegie Endowment for International Peace, 2016, https://carnegieendowment.org/files/12-16-16_Russia_and_Cyber_Operations.pdf (accessed 13 March 2023); Booz Allen Hamilton, "Bearing witness. Uncovering the logic behind-Russian military cyber operations", 2020, https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html (accessed 13 March 2023); Congressional Research Service "Russian Cyber Units", *In Focus* no. 11718 (Updated 2 February 2022), https://crsreports.congress.gov/product/pdf/IF/IF11718 (accessed 13 March 2023); and National Cyber Security Centre, "Reckless campaign of

example, we can read analyses of incidents such as Moonlight Maze, NotPetya, or BlackEnergy, or groups such as 16th Centre (Field Post No. 71330, *Berserk* Bear), APT 28 (*Fancy Bear*), APT 29 (Field Post No. 26165, *Cozy Bear*), or the Turla group.[99]

Focussing on the development of governance, Andrei Soldatov and Irina Borogan explain how and where Russian federal cyber power has been directed to. Despite (or perhaps because of) a wide range of state and non-state, political and security actors dealing with information security issues, Russia does not have a unified cyber command. Efforts to establish one were announced in the early 2010s. Soldatov and Borogan note that cyber capabilities and operations in the Russian military are developed and run by two directorates within Russian General Staff Main Intelligence Directorate (GU, also GRU): the 6th and the 8th Directorate. They conclude that the political element has played a decisive role in Russian cyber or information warfare activities. In particular, the Presidential Administration and the Security Council have directed efforts, but the Moscow State University Institute for Information Security Issues has also had an influential role in formulating concepts, principles, and policies. Most importantly, the Federal Security Service (FSB) is claimed to have sidelined the General Staff in the development of federal cyber concepts and capabilities.[100] As a result, Russian federal cyber power reflects the threat perceptions and domestic policy ambitions of the ruling regime rather than the provision of military cyber capabilities to combatant commanders.

The 2010 Chinese defence white paper explained informationization as part of the modernisation of the People's Liberation Army (PLA). Theoretical studies and the development of high-tech weapons and equipment, as well as new types of combat forces and joint operations, were meant to provide and accelerate the transition of "a new type of combat capability to win local wars in conditions of informationization, [strengthen] the composite development of mechanisation and informationization with the latter as the leading factor, [focus] informationization on raising its fighting capabilities based on information systems, and [enhance] the capabilities in fire power, mobility, protection, support and informationization." This ambition can still be read as digitalisation of the battlefield and its main tools and processes, rather than building military capabilities for cyber operations. Indeed, the notion of "cyber" was mentioned in negative fashion, noting that some powers develop doctrinal and operational capability "to occupy new strategic commanding heights."[101]

China's 2015 military strategy reaffirmed cyberspace as enabling the occupation of new commanding heights[102] in strategic competition and noted a general development of

cyber-attacks by Russian military intelligence service exposed", 3 October 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed 13 March 2023).

[99] See, The European Repository of Cyber Incidents "APT Profiles" for analysis of Advanced Persistent Threat groups, including the here-mentioned APT 28 (*Fancy Bear*) and APT 29 (*Cozy Bear*) (https://eurepoc.eu/apts).

[100] Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, Center for European Policy Analysis (2022): 4–5, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/ (accessed 13 March 2023). My encounters with Russian Security Council, Ministry of Foreign Affairs, Moscow State University, and General Staff personnel support Soldatov's and Borogan's conclusions. It appears that the Russian Ministry of Defence has managed to enhance its cyber competence through expanded military technological education and scientific and operational research. Still, military cyber capacity - capabilities to support combatant commanders with intelligence, offensive, or defensive network operations – seems not to exist.

[101] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2010*, 31 March 2011, http://www.china.org.cn/government/whitepaper/node_7114675.htm (accessed 13 March 2023).

[102] The expression of "the commanding heights" is explicitly expressed in the Howard & Paret edition and translation of *On War*, Book 5:18. The chapter, titled in German as *Überhöhen,* elaborates on elevated and dominating positions, especially heights, in warfare and art of war. Sun Tzu, *The Art of War,* chapter 10,

military cyber forces. As cyberspace was seen as more important to military security, China was said to "expedite the development of a cyber force", including the enhancement of cyberspace situational awareness and cyber defence. Commanding the heights is an enabler but also a risk. The development of Chinese cyber capacity was also to "ensure national network and information security and maintain national security and social stability."[103]

Established in 2016, the Strategic Support Force (SSF) has integrated aerospace, cyberspace, and electronic warfare, fulfilling the ideal of integrated joint operations (*yiti lianhe zuozhan*) and integrated network electronic warfare (*wangdian yitizhan*) that General Dai Qingmin, the former PLA Fourth Department commander, had advocated for. The establishment of the SSF under the direct command of the Central Military Committee underlines the Communist Party's control and the role political interests play in information warfare.[104] The SSF Network Systems Department is responsible for achieving information dominance through strategic information superiority, including offensive cyber warfare and information support services to theatre military commands, making it a Chinese equivalent of a cyber command.[105]

Chinese cyber or informational capabilities are no more exceptional than anyone else's. The imperative of winning informationised local wars, as well as the integration of combat forces in system-against-system operations involving information dominance, precision strikes, and joint operations,[106] could not be achieved without offensive cyber capabilities.

In practise, development and operations of the Chinese military cyber capability have focussed on cyber espionage rather than effects-creating operations. The difference with Russian *modus operandi* should not go unnoticed. The difference from US ambitions to develop deployable and organic battlefield capabilities also seems clear – at least until the People's Liberation Army is engaged in a war and its battlefield and deployable military cyber capabilities are employed.[107] As Chang concluded, the Chinese Communist Party's primary goal is "maintaining its governing power."[108] This is in line with communist and totalitarian fashion and is also clearly outlined in the 2015 military strategy.

Matthias Schulze and Mika Kerttunen have identified three partly successive, partly parallel strands in the development of military cyber doctrines and units. The strategic cyber warfare narrative of the 1990s saw cyber warfare as a next-generation front that would threaten modern society with digital decapitation attacks that would bring entire economies to a standstill, all without the need for physical military force. Within this narrative,

"Configurations of Terrain" similarly oscillates between the concrete and the metaphorical, but implicitly focusses of the tactical utility and strategic significance of precipitous heights, too. See also, Sun Tzu, chapter 9, "Maneuvering the Army" (Ralph D. Sawyer, *The Seven Military Classics of Ancient China* (New York: Basic Books, 2007)).

[103] The State Council Information Office of the People's Republic of China, *China's Military Strategy*, 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (accessed 13 March 2023).

[104] Nigel Inkster, "China's Cyber Power", *The Adelphi Series,* no. 456 (2016); Ying-Yu Lin, "PLA Cyber Operations: A New Type of Cross-Border Attack", in *The PLA Beyond Borders. Chinese Military Operations in Regional and Global Context,* ed. Joel Wuthnow, Arthur S. Ding, Phillip C. Saunders, Andrew Scobell, and Andrew N.D. Yang (Washington, D.C., National Defense University Press, 2021): 295–310. Also, Amy J. Nelson and Gerald L. Epstein "The PLA's Strategic Support Force and AI Innovation", *Tech Stream*, 23 December 2022, https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/ (accessed 13 March 2023). Whereas Ying-Yu Lin lists electronic and electromagnetic warfare and intelligence within the SSF areas of responsibility, Nelson and Epstein do not, but add psychological warfare.

[105] Nelson and Epstein, "PLA", (see note 104).

[106] The State Council Information Office, *China's Military Strategy* (see note 103).

[107] Observing cyber exercises may provide additional information on national capacities and doctrines. On the other hand, carefully constructed exercises and controlled events may offer either limited or exaggerated insight.

[108] Chang, *China's Cybersecurity Strategy* (see note 59): 8, 10, 32.

cyber operations were seen as a strategic countervalue capability that would target societies with the aim of influencing state behaviour in peacetime. In short, cyber operations were expected to change the balance of power in the international system because they were perceived to be superior to conventional force. Second, cyber operations began to be seen as force enablers/multipliers for conventional military operations and capabilities, especially when used in a joint and combined manner. In this view, cyber operations in war are not necessarily measured by their strategic effects, but rather as a counterforce capability that can be directed against enemy armies. Third, cyber is not recognised as a primary destructive force in war, but rather as optimal for grey zone activities between peace and war. The essential modus operandi is not to disable armies, but to subvert, exploit, and shape the cyber and information environment in an information contest or strategic competition. The main utility of cyber operations is seen as the theft or manipulation of information for political, economic, or even criminal purposes.[109]

Although some in the Western military-intelligence complex may yearn for Russian and Chinese-style peacetime operational boldness or executive intervention capacity, the Russian and Chinese-style practices would only increase the space and extraordinary authority of the executive over the legislative and judicial branches, undermining the very foundations of liberal democracies. Moreover, peacetime cyber intelligence and offensive operations will increase the risk of misinterpretation and unintended escalation.

[109] Matthias Schulze and Mika Kerttunen, "Cyber Operations in Russia's War against Ukraine", *SWP Aktuell* no. 23, April 2023 (forthcoming).

Military cyber units

Based on their main purpose and function, military units can be divided into three broad categories: commands and headquarters, combat units, and supporting units. Following the original US concepts of joint functions, a more nuanced distinction speaks of "seven basic groups of command and control, information, intelligence, fires, movement and manoeuvre, protection, and sustainment."[110] A comprehensive capability development perspective includes such capability elements as laws and policies, human resources, and finances.[111] Clearly, the development of national and military cyber prowess and units requires a broad category of capabilities. For example, in 2014, the then-commander of the U.S. Cyber Command, Admiral Michael Rogers, explained how the Cyber Command's greatest challenge to becoming viable as a military domain required the capabilities of truly defensible networks, common situational awareness, authority and responsibility to act, operational concepts and a command-and-control structure, and trained and deployable forces.[112]

Some countries have established cyber commands to plan and lead operations. There is no universal understanding or shared practice that constitutes a cyber command. Linguistically, a military command refers to a position of supreme authority (within a specific field, area, or domain), as well as to the ability or power to control or exercise dominating influence, mastery;[113] doctrinally, as defined by the Pentagon, a command refers to "a unit or units, an organization, or an area under the command of one individual."[114] The military units, which may or may not be called cyber commands, exercise highest authority within their field; that is *command* by planning, directing, coordinating, and representing the cyber domain or area within joint or combined headquarters and commands.[115]

National practices for establishing and designating military cyber units vary. First, the aforementioned US joint cyberspace operations doctrine recognises cyberspace operations forces under the direct command of commander, the U.S. Cyber Command, and under the respective commanders of the Army, Navy, Air Force, and Marine Corps. For each mission, the assigned or attached units are organised as a Cyber Mission Force. The Services comprise the three elements of the Cyber Mission Force, with tasks reflecting the outlined DOD missions of defending, responding to incidents, and protecting critical infrastructure.

The Cyber Protection Force, consisting of Cyberspace Protection Teams, defends assigned cyberspace and conducts internal protection of the DOD Information Network; the Cyber National Mission Force, consisting of National Mission Teams, National Support Teams, and national-level Cyberspace Protection Teams, conducts cyberspace operations to defeat significant cyberspace threats to the DOD Information Network "and, when ordered, to the nation"; and the Cyber Combat Mission Force conducts cyberspace operations to support the missions, plans, and priorities of the geographic and functional Combatant Commanders.[116]

[110] Joint Chiefs of Staff, *DOD Dictionary* (2019).

[111] Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations,* Enclosure F (2006).*;* Stephan De Spiegeleire, "Ten Trends in Capability Planning for Defence and Security", *The RUSI Journal,* 156:5 (2011): 20–28, http://dx.doi.org/10.1080/03071847.2011.626270); Smeets, *No Shortcuts* (see note 82).

[112] U.S. Department of Defense, "Operationalizing Cyber is New Commander's Biggest Challenge", *American Forces Press Service* (2 June 2014).

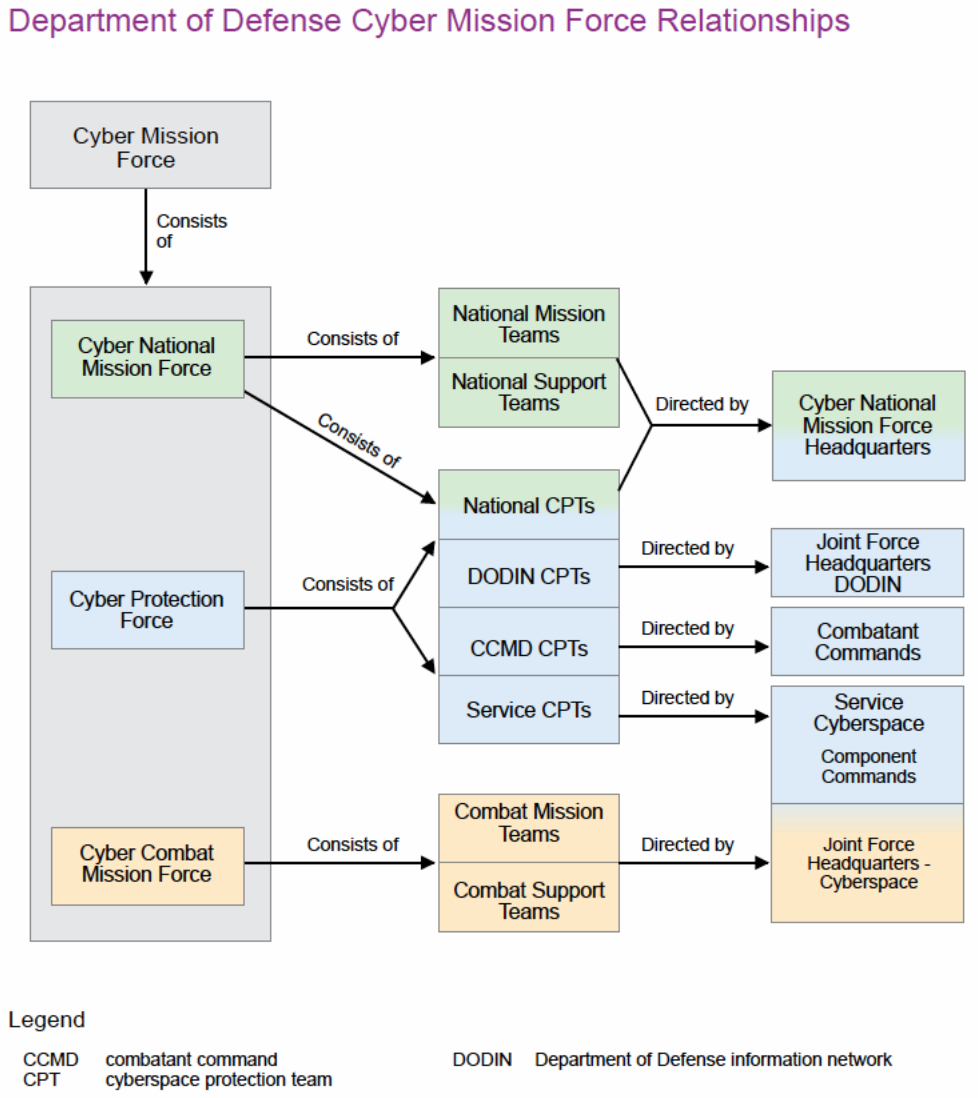
[113] *Longman Webster English College Dictionary*, 1st edition (1984).

[114] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (2019).

[115] See, Piret Pernik, "National Cyber Commands", in *Routledge Handbook of International Cybersecurity*, ed. Mika Kerttunen & Eneken Tikk (Abingdon: Routledge, 2020): 186–198.

[116] *JP 3-12* (see note 93): I-8 – I-9.

The following figure illustrates the U.S. Department of Defense Cyber Force Mission structure and relationships across various levels of military commands and headquarters.



Department of Defense Cyber Mission Force Relationships
Cyber Mission Force
Consists of
Cyber National Mission Force
Consists of
National Mission Teams
National Support Teams
Directed by
Cyber National Mission Force Headquarters
Consists of
National CPTs
DODIN CPTs
Directed by
Joint Force Headquarters DODIN
Cyber Protection Force
Consists of
CCMD CPTs
Directed by
Combatant Commands
Service CPTs
Directed by
Service Cyberspace Component Commands
Cyber Combat Mission Force
Consists of
Combat Mission Teams
Combat Support Teams
Directed by
Joint Force Headquarters - Cyberspace
Legend
CCMD combatant command
CPT cyberspace protection team
DODIN Department of Defense information network

Figure 3. The U.S. Department of Defense Cyber Mission Force Relationships.
Source: Joint Chiefs of Staff, *Cyberspace Operations, JP 3-12* (8 June 2018), p. I-10.

For the purposes of analysing of the employment of military cyber capabilities in war, *military cyber units* are understood as *units designated to conduct cyberoperations in and through cyberspace*. As noted above, Jason Blessing similarly categorises cyber force in a similar fashion "as active-duty military organizations with the capability and authority to direct and control strategic cyberspace operations to influence strategic diplomatic and/or military interactions." Following the hierarchical classification of military force structure, labelled as "organizational model", he correctly distinguishes joint, service, and branch level units. In a perhaps less informative way, he also distinguishes the "scale of command", the unified, sub-unified, and subordinated commands, or units, resulting in a combination of nine different force structures.[117] It is fair to say that each national force structure is unique, but for academic and professional purposes, as well as for the sake of clarity and distinction, the following table identifies military cyber units in five joint function categories. The organisational-hierarchical setting "comes on top."

Common military functions	**Activities**	**Examples of military cyber units**
Command and Control/Leadership	Planning, directing, and leading operations and all other activities	National cyber commands Service cyber commands Information operations commands
Intelligence	Gathering, analysing, and disseminating intelligence information to support decision-making	Military intelligence groups, brigades, battalions, and companies Intelligence centres Advanced Persistent Threat hacking groups
Operations/Fires, manoeuvres, protection	Conducting the core combat and combat support mission and tasks of the specific unit in question	Armed forces operations centres Cyber warfare battalions Cybersecurity companies Deployable cyber warfare and protection teams
Logistics/Sustainment	Ensuring the continuity operations and other activities through timely and targeted flow of materiel, support, and services	Depots and warehouses, transportation, and maintenance military units and civilian suppliers of digital and non-digital materiel and services
Communications/Communication and Information Systems	Establishing and maintaining global and local communication and information systems	Defence information system agencies and commands Network commands Signal battalions

Table 2. Military cyber units in five joint function categories. Author's compilation.

It is also fair to say that the core cyber, or cyberspace, operation-specific military (armed forces) groups and units conduct intelligence, defensive, or offensive computer network operations. Cyber operations employ cyber (digital) means to exploit or affect digital data or information and communication systems and services. The employment of digital assets, such as sensor images, computing, or artificial intelligence or devices such as smart phones, positioning systems, or electronic jammers to support "kinetic", logistic, or cognitive-psychological operations does not constitute cyber operations. This differentiation of operations follows the US joint cyberspace operations doctrine (2013 and 2018), which makes the above-explained distinction between cyberspace and information operations. Reality, however, is not that clear cut.

The U.S. Army Cyber Command, for example, is said to integrate information, electromagnetic warfare, and cyberspace operations to influence relevant actors. Its 915th Cyber Warfare Battalion trains and deploys Expeditionary Cyber Teams, which provide offensive information and cyber operations and electronic warfare capabilities to tactical units.

[117] Blessing, "Cyber Forces" (see note 80).

Moreover, the Cyber Command has Theater IO Groups, a Civil Affairs & Psychological Operations Command, and an Information Operations Command.[118]

Moreover, the technological distinction between computer network operations and electronic warfare is diminishing. Similarly, the distinction between civilian and military effect-creating cyber operations is blurring. In particular, civilian intelligence and security agencies conduct standalone cyber operations and cyber operations in the context of armed conflict.

To summarise the discussion on the nature or characteristics of military cyber units, Table 3 below provides examples of military cyber units with their main operational tasks that some countries have established. In addition to operational tasks, many commands and units have doctrinal and organisational development as well as training, education, and exercise responsibilities.[119]

[118] U.S. Army Cyber Command, "Our Units", https://www.arcyber.army.mil/Organization/Units/ (accessed 13 March 2023).

[119] One should notice that both publicly-available official information and research information can be tainted and limited by secrecy and unavailability of complete and truthful knowledge.

Country	Unit	Main tasks
US	U.S. Cyber Command	To defend the DoDIN, support to combatant commanders, and to strengthen the national ability to withstand and respond to cyber-attacks. To design the cyber force structure, training requirements, and certification standards that will enable the Services to build the cyber force required to execute our assigned missions.[120]
	Cyber National Mission Force	To defend the nation in cyberspace through offensive, defensive, and information operations. The mission of CNMF is to plan, direct, and synchronize full-spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber and malign actors. The organization supports the national mission and U.S. Cyber Command priorities, such as election security, ransomware, cyber espionage, and other crises and contingencies.[121]
	U.S. Army Cyber Command	To integrate and conduct cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and throughout the cyber domain and the information dimension, while denying the same to adversaries.[122]
	11th Cyber Battalion	To train and deploy Expeditionary Cyber Teams (ECT) to augment corps and lower units. The ECTs provide offensive Cyber, IO, and EW capabilities not currently fielded to tactical units.[123]
RU	Main Intelligence Administration (*Glavnoye Razvedyvatelnoye Upravlenie* (GRU))	Political, military, economic and societal intelligence through human, signals, and electronic and network intelligence to support decision-making, and to prepare and support Russian military operations abroad using operational-tactical intelligence gathered on the target country. [124]
	GRU Unit 26165	Reconnaissance support to cyber operations, network intrusion, cyber espionage, and data destruction.[125]
CN	Strategic Support Force (SSF)	To support battlefield operations by providing information and strategic support to form an "information umbrella" for joint operations and other services, including network attack and defence, electronic warfare, provision of intelligence, surveillance, reconnaissance and navigation support, and defence of the cyber domain and electromagnetic spectrum.[126]
	SSF Network Systems Department SSF Space Systems Department	
	PLA Unit 61398 (a.k.a. APT 1)	Network intrusion, protracted cyber operations, cyber espionage, social engineering, and spearphishing.[127]

Table 3. Examples of military cyber units and their main operational tasks. Author's compilation from the footnoted sources.

[120] U.S. Cyber Command, "Our mission and values", https://www.cybercom.mil/About/Mission-and-Vision/ (accessed 13 March 2023).

[121] U.S. Cyber Command, "Cyber National Mission Force (CNMF)", https://www.cybercom.mil/About/Components/CNMF/, (accessed 13 March 2023).

[122] U.S. Army Cyber Command, "Our mission", https://www.arcyber.army.mil/ (accessed 13 March 2023).

[123] U.S. Army Cyber Command, "Our units", https://www.arcyber.army.mil/Organization/Units/ (accessed 13 March 2023).

[124] Global Security, "Operations of the Main Intelligence Administration (GRU)", https://www.globalsecurity.org/intell/world/russia/gru-ops.htm (accessed 13 March 2023).

[125] Atlantic Council, "GRU 26165: The Russian cyber unit that hacks targets on-site", 18 November 2022, https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-russian-cyber-unit-that-hacks-targets-on-site/ (accessed 13 March 2023).

[126] Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica: RAND, 2017), p. 13–16, https://www.rand.org/pubs/research_reports/RR2058.html (accessed 13 March 2023).

[127] Council on Foreign Relations, *PLA Unit 61398* (2023), https://www.cfr.org/cyber-operations/pla-unit-61398 (accessed 13 March 2023).; Mandiant, *APT 1. Exposing One of China's Cyber Espionage Units* (2013), https://web.archive.org/web/20130219155150/http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed 13 March 2023).

Country	Unit	Main tasks
DE	Cyber and Information space Command (*Kommando Cyber- und Informationsraum*)	To develop the area of cyber and information security of the Bundeswehr and the training and further education of its staff. To serve as the office of the Inspector CIR (Cyber- und Informationsraum) and Chief Information Security Officer; tasked with carrying the overall responsibility for the information security of the Bundeswehr.[128]
	Strategic Reconnaissance Command (*Kommando Strategische Aufklärung*)	To obtain information for early crisis detection and to support operations for the purpose of providing decision-makers with usable information in good time. The range of tasks and capabilities includes satellite-based imaging reconnaissance, communications and electronic reconnaissance, electronic warfare, and object analysis, as well as telecommunications reconnaissance and interference with electromagnetic radiation The ability to conduct computer network operations is still being developed.[129]
	Cyber Operations Centre (*Zentrum Cyber-Operationen*)	To plan, prepare, manage, and conduct reconnaissance and effect-creating operations in the context of national and alliance defence and in mandated deployments of the Bundeswehr. In addition to being responsible for offensive and defensive CO, forces at the ZCO Centre can conduct cyber operations within the framework of IT incidents.[130]
NO	Cyber Defence *(Cyberforsvaret)*	To deliver ICT and C2 systems and services to the Defence Forces (NDF) units at home and abroad, to operate and maintain NDF C2 infrastructure, to defend NDF C2 and ICT systems from digital threats and cyber-attacks, and to maintain NDF freedom of manoeuvre in cyber domain.[131]
	Cyber Security Centre (*Cybersikkerhetssenteret*)	To detect and analyse digital threats against the NDF operations and ICT and C2 systems, to lead defensive cyber operations in support of the NDF operational activities, and to offer force protection to NDF operational headquarters from digital disruption, degradation, and sabotage.[132]
EE	Cyber Command (*Kyberkaitseväejuhatus*)	To carry out operations in cyberspace to provide command support for the Ministry of Defence's area of responsibility, including support for ICT infrastructure and services, cyber defence, planning and execution of cyber operations, information operations, and strategic communications; also tasked with gaining, maintaining, and sharing cyberspace situational awareness.[133]
	STRATCOM Centre	To support media operations with video and photo materials and their transmission to the media or publication sections of the Defence Forces communication channels, and to support direct communication projects organised for media communication channels.[134]

Table 3 continued. Examples of military cyber units and their main operational tasks. Author's compilation from the footnoted sources.

[128] Kommando Cyber- und Informationsraum, *Auftrag*, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum (accessed 14 March 2023).

[129] Kommando Strategische Aufklärung, *Auftrag*, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung (accessed 14 March 2023).

[130] Zentrum Cyber-Operationen, "Auftrag" (2323), https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung/zentrum-cyber-operationen (accessed 14 March 2023).

[131] Cyberforsvaret [Cyber Defence], "Oppgaver" [Tasks] (2023), https://www.forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret (accessed 14 March 2023).

[132] Cyberforsvaret [Cyber Defence], "Avdelninger" [Section*s*] (2023), https://www.forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret.

[133] Estonian Defence Forces, "Cyber Command" (2023), https://mil.ee/en/landforces/cyber-command/ (accessed 14 March 2023).

[134] Estonian Defence Forces, "Cyber Command: Strategic Communications Centre" (2023), https://mil.ee/en/landforces/cyber-command/#t-strategic-communications-centre (accessed 14 March 2023).

Part 3. *Expressionism.* Cyber warfare in Ukraine 2022

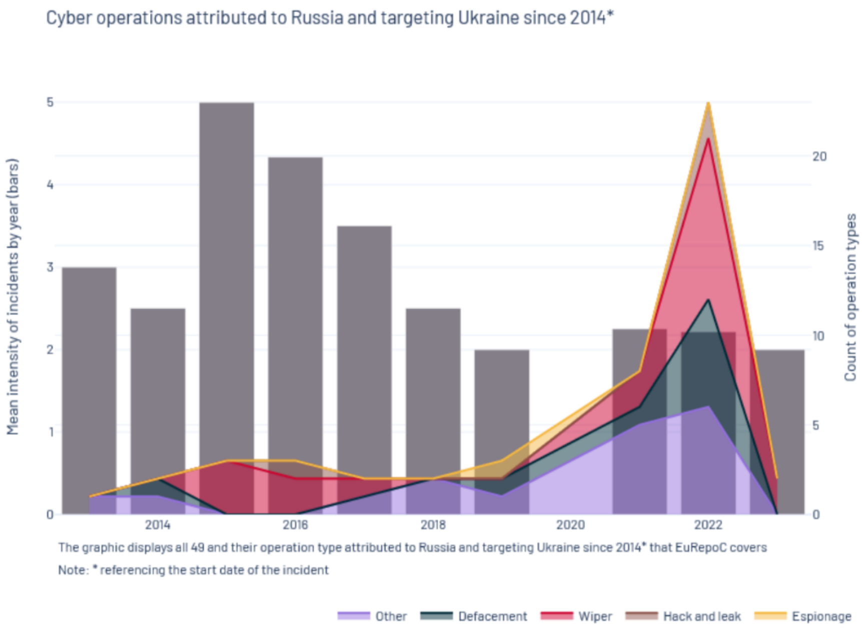
> *"If a decision by fighting is the basis of all plans and operations, it follows that the enemy can frustrate everything through a successful battle."*
>
> *Carl von Clausewitz, Vom Kriege (Book 1, Chapter 2)*

Russian cyber activities

Quite early in the war, during Russian re-invasion of Ukraine in February 2022, corporate reports and blog posts began to tell the story of many cyber-attacks against Ukrainian state and societal targets. Russian intelligence preparation of the battlefield[135] began long before the February 2022 offensive commenced. One does not need to go back to the Orange Revolution of 2004 or the Euromaidan demonstration of 2014 to see continued Russian intelligence interest or network and information operations against Ukraine.[136] It may be impossible to precisely answer how much of the Russian activities were part of the preparation for an overt military offensive; however, it is clear that Russian network and information intensified in quality and quantity in late 2021 and early 2022. The volume and types of Russian cyber-attacks against Ukraine in 2014-2022, and more specifically between November 2021 and January 2023 are illustrated as a function of their chronological distribution in the following charts (Figure 4, and Figure 5, respectively).

[135] The notion in general refers to a systematic process of gathering and analysing the operational variables of an adversary, its political, military, and technical systems, and their strengths and weaknesses, but also variables such as (physical) terrain, weather, and diplomatic and civilian considerations to determine an optimal conduct of operations. See, for example, Headquarters, Department of Army, *Intelligence Preparation of the Battlefield.* ATP 2-01.3 (2019), https://home.army.mil/wood/application/files/8915/5751/8365/ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield.pdf (accessed 14 March 2023). See, also Jen Weedon, "Beyond 'Cyber War': Russian Use of Strategic Espionage and Information Operations in Ukraine", in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCDCOE, 2015): 67–78.

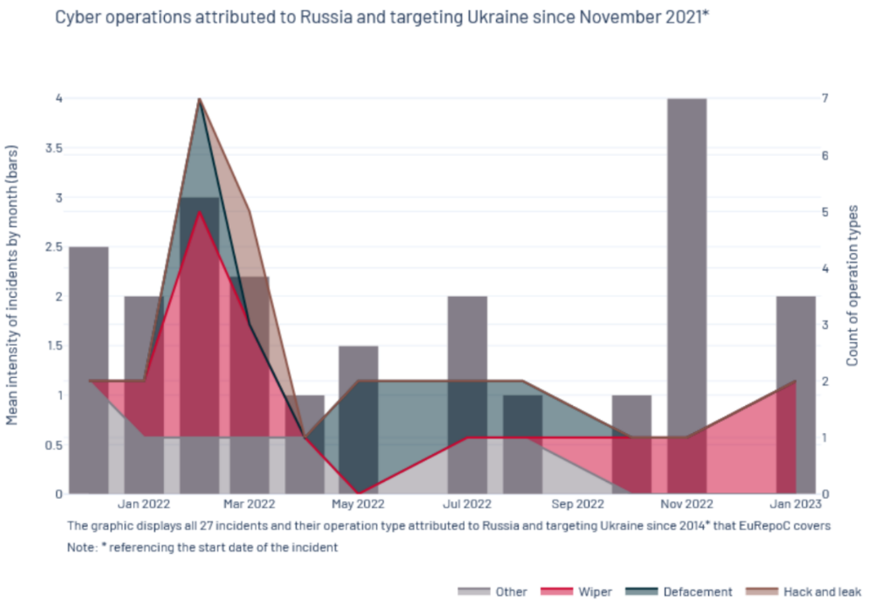
[136] Russo-Ukrainian dispute, conflict, and war has been analysed and presented in various timelines. See, for example, Belfer Center, "Understanding the Turmoil in Ukraine" (2014), https://www.belfercenter.org/publication/understanding-turmoil-ukraine (accessed 14 March 2023); House of Commons, *Conflict in Ukraine: A timeline (2014 – present), Research Briefing* (24 February 2023), https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf (accessed 14 March 2023); and European Council, "Timeline - EU response to Russia's invasion of Ukraine" (2023), https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/timeline-eu-response-ukraine-invasion/ (accessed 14 March 2023).


Cyber operations attributed to Russia and targeting Ukraine since 2014*

The graphic displays all 49 and their operation type attributed to Russia and targeting Ukraine since 2014* that EuRepoC covers

Note: * referencing the start date of the incident

Figure 4. The amount and types of Russian cyber-attacks against Ukraine since 2014 as a function of their chronological distribution. Data: EuRepoC.[137] Data analysis: Jonas Hemmelskamp.


Cyber operations attributed to Russia and targeting Ukraine since November 2021*

The graphic displays all 27 incidents and their operation type attributed to Russia and targeting Ukraine since 2014* that EuRepoC covers

Note: * referencing the start date of the incident

Figure 5. The amount and types of Russian cyber-attacks against Ukraine since November 2021 as a function of their chronological distribution. Data: EuRepoC. Data analysis: Jonas Hemmelskamp.

[137] The *European Repository of Cyber Incidents* (EuRepoC), an independent research consortium dedicated to providing evidence-based scientific analysis of cyber incidents. Data collection, inclusion criteria, and analysis methodology is explained, and the data is available at https://eurepoc.eu/.

In early 2022, alongside increasing Russian troop concentrations, Russian phishing efforts attempted to gain access to emails and networks, and subsequently sensitive information. The APT group Nobelium, linked to the Russian intelligence service (SVR), was identified as one actor. Russian state actors or affiliated groups had continued to attempt to compromise communications, transportation, energy, defence, and administrative and diplomatic systems and services throughout 2021.[138] Groups originating from the Federal Security Service (FSB) were also involved in Russian cyber-attacks and intelligence activities against Ukraine.[139]

On February 23, 2022, the day before the military campaign began, the Russian military intelligence agency, GRU, launched several destructive data-wiping attacks on Ukrainian government, IT, energy, and financial organisations, apparently in support of the coming ground and air assaults. Unit 74455, also known as Iridium and Sandworm, was identified as one of the attackers.[140] Figure 6 illustrates the timing of the Russian cyber and military activities from winter to spring 2022. It is important to note that many of the Russian conventional military attacks have targeted civilian and societal targets without any direct significance to ongoing tactical or operational manoeuvres. In other words, military and civilian activities, as well as so-called kinetic and virtual use and projection of harmful or destructive means, do not follow the boundaries of domains or, unfortunately, the categories of lawful and unlawful targets.

[138] Microsoft, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* (22 April 2022): 5–7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (accessed 14 March 2023); Google, "Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape" (16 February 2023): 6–12, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (accessed 14 March 2023).

[139] European Repository of Cyber Incidents, "Gamaredon Russian Intelligence Preparation of the Battlefield in Ukraine", *Advanced Persistent Threat profile* (January 2023), https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Gamaredon_13d3d3be46.pdf (accessed 14 March 2023).

[140] Microsoft, *Special Report* (see note 138); Google, "Fog of War" (see note 138).

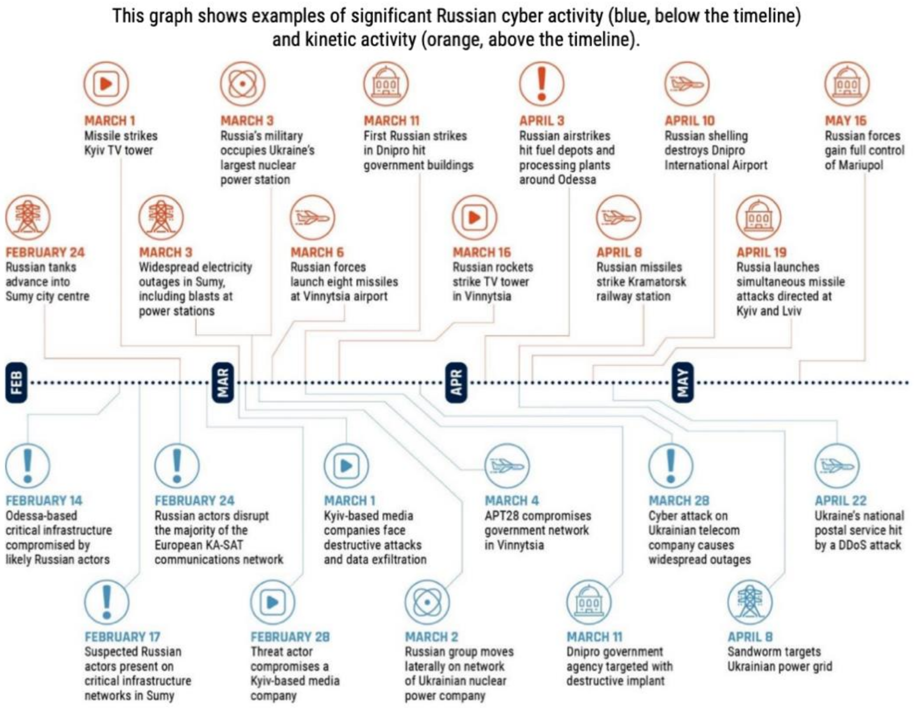

This graph shows examples of significant Russian cyber activity (blue, below the timeline) and kinetic activity (orange, above the timeline).
MARCH 1 Missile strikes Kyiv TV tower
MARCH 3 Russia's military occupies Ukraine's largest nuclear power station
MARCH 11 First Russian strikes in Dnipro hit government buildings
APRIL 3 Russian airstrikes hit fuel depots and processing plants around Odessa
APRIL 10 Russian shelling destroys Dnipro International Airport
MAY 16 Russian forces gain full control of Mariupol
FEBRUARY 24 Russian tanks advance into Sumy city centre
MARCH 3 Widespread electricity outages in Sumy, including blasts at power stations
MARCH 6 Russian forces launch eight missiles at Vinnytsia airport
MARCH 16 Russian rockets strike TV tower in Vinnytsia
APRIL 8 Russian missiles strike Kramatorsk railway station
APRIL 19 Russia launches simultaneous missile attacks directed at Kyiv and Lviv
FEB
MAR
APR
MAY
FEBRUARY 14 Odessa-based critical infrastructure compromised by likely Russian actors
FEBRUARY 24 Russian actors disrupt the majority of the European KA-SAT communications network
MARCH 1 Kyiv-based media companies face destructive attacks and data exfiltration
MARCH 4 APT28 compromises government network in Vinnytsia
MARCH 28 Cyber attack on Ukrainian telecom company causes widespread outages
APRIL 22 Ukraine's national postal service hit by a DDoS attack
FEBRUARY 17 Suspected Russian actors present on critical infrastructure networks in Sumy
FEBRUARY 28 Threat actor compromises a Kyiv-based media company
MARCH 2 Russian group moves laterally on network of Ukrainian nuclear power company
MARCH 11 Dnipro government agency targeted with destructive implant
APRIL 8 Sandworm targets Ukrainian power grid

Figure 6. Timeline of some Russian cyber and military activities in winter – spring 2022. Source: Canadian Centre for Cyber Security, "Cyber Threat Activity Related to the Russian Invasion of Ukraine", *Cyber Threat Bulletin* (2022), p. 3.

For example, although an April 2022 Microsoft report found that Russian APTs are conducting intrusions in concert with kinetic military actions,[141] the different types of attacks do not appear to be well-conducted. Many observers suggest the opposite. James Lewis, for example, bluntly states that "all these hacking efforts, whether by the GRU or not, seem to have been poorly coordinated with Russian military actions in Ukraine."[142] Gavin Wilde notes that, while the most advanced military cyber forces are still wrestling with how to effectively integrate cyber into conventional military operations, "Russia doesn't appear to have done so thus far."[143] Jon Bateman also concludes that "Russia seems unwilling or unable to plan and wage war in the precise, intelligence-driven manner that is optimal for cyber operations."[144]

On the other hand, the Canadian Centre for Cyber Security (CCCS) assesses that Russian cyber operations have "almost certainly" sought to degrade, disrupt, destroy, or discredit

[141] Microsoft, *Special Report* (see note 138): 2–5, 8, 10.

[142] James Lewis, *Cyber War and Ukraine* (Center for Strategic and International Studies, June 2022): 1–3. Lewis also notes how militarily insignificant private sector attacks against Russian websites have been. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash (accessed 14 March 2023).

[143] Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare", Carnegie Endowment for International Peace, 19 November 2022, https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 (accessed 14 March 2023).

[144] Jon Bateman, "What the Russian Invasion Reveals About the Future of Cyber Warfare" (Carnegie Endowment for International Peace, 19 November 2022). https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 (accessed 14 March 2023).

Ukrainian government, military, and economic functions; they have also sought to secure footholds in critical infrastructure and limit the Ukrainian public's access to information.

The CCCS notes that several attacks have spilled over into other countries, such as one that disrupted Viasat European KA-SAT satellite communications service networks in late February and early March 2022. The CCCS also estimates that Russian state-sponsored cyber threat actors will most likely continue to conduct actions in support of the Russian armed forces' strategic and tactical objectives in Ukraine.[145]

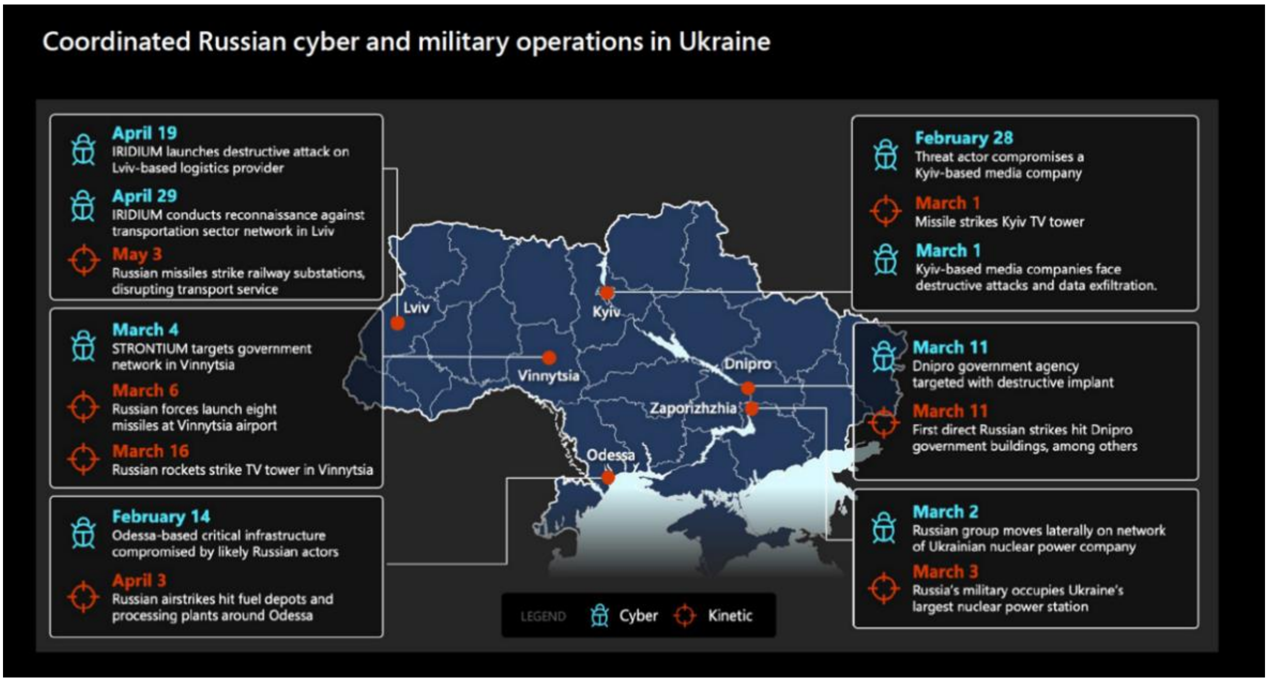
Bateman concludes that intelligence collection for pre-war planning was probably Russia's main cyber activity in Ukraine.[146] This finding is circumstantially supported by the fact that Russia appears to have been willing and able to destroy Ukrainian infrastructure through shelling. Notwithstanding the importance of intelligence-gathering, Russia has conducted a significant number of destructive attacks on data, most likely to freeze Ukrainian government and military decision-making. In addition, distributed denial of service (DDoS) attacks can also be considered to be effect-creating, as they block access and availability of services and the data within. The effectiveness of DDoS *anno 2022* compared to *Estonia 2007* can be debated, especially in the light of the Cyber Peace Institute's estimate that 71.3 and 87.3% of all incidents originating in Russia were distributed denial of service attacks (Q3 and Q4, respectively).[147]

[145] Canadian Centre for Cyber Security, "Cyber Threat Activity Related to the Russian Invasion of Ukraine", *Cyber Threat Bulletin* (2022), https://cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf (accessed 14 March 2023). An April 2022 report from Microsoft, too, identifies destructive attacks as being a prominent component of Russian cyber operations (Microsoft, *Special Report* [see note 138]).

[146] Bateman, "Russian Invasion" (see note 144).

[147] Cyber Peace Institute, *Cyber Dimensions of the Armed Conflict in Ukraine.* Quarterly Analysis. Q3, and Q4 October to December 2022 (16 December 2022 and 1 February 2023): 4, https://cyberpeaceinstitute.org/research-and-investigations (accessed 14 March 2023).

Russian cyber-attacks targeted the same organisations and services as conventional military fire, missiles, rockets, and bombs. Just as a government's data was hit by missiles, the government's on-premises computer networks were targeted by destructive data wiping cyber-attacks.[148] Microsoft notes that Russian cyber-attacks succeeded in disrupting technical services and creating a "chaotic information environment." However, it claims to be unable to evaluate the broader strategic impact of the Russian cyber and information operations, such as the erosion of confidence and the capacities of Ukrainian military defence.[149] Global, regional, and local information operations using cyber means, social media platforms, print, and broadcast media, as well as multilateral and bilateral diplomacy, fulfil the Russian spectrum of state power projection. The map below illustrates the coordination of cyber and military operations.



Coordinated Russian cyber and military operations in Ukraine

April 19
IRIDIUM launches destructive attack on Lviv-based logistics provider

April 29
IRIDIUM conducts reconnaissance against transportation sector network in Lviv

May 3
Russian missiles strike railway substations, disrupting transport service

March 4
STRONTIUM targets government network in Vinnytsia

March 6
Russian forces launch eight missiles at Vinnytsia airport

March 16
Russian rockets strike TV tower in Vinnytsia

February 14
Odessa-based critical infrastructure compromised by likely Russian actors

April 3
Russian airstrikes hit fuel depots and processing plants around Odessa

February 28
Threat actor compromises a Kyiv-based media company

March 1
Missile strikes Kyiv TV tower

March 1
Kyiv-based media companies face destructive attacks and data exfiltration.

March 11
Dnipro government agency targeted with destructive implant

March 11
First direct Russian strikes hit Dnipro government buildings, among others

March 2
Russian group moves laterally on network of Ukrainian nuclear power company

March 3
Russia's military occupies Ukraine's largest nuclear power station

Figure 7. Examples of the coordinated Russian cyber-attacks and military strikes in Ukraine in March and April 2022. Source: Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (27 June 2022), p. 2, 5, 7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[148] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (27 June 2022): 2, 5, 7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK (accessed 14 March 2023).
[149] Microsoft, Special Report (see note 138): 2–5, 8, 10. Bateman similarly concludes that "no subsequent Russian cyber-attack has had visible effects of comparable military significance" (Bateman, "Russian Invasion" (see note 144)). Carnegie Endowment for International Peace, "What the Russian Invasion Reveals About the Future of Cyber Warfare" (19 December 2022), https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 (accessed 14 March 2023).

The joint Google and Mandiant analysis identifies five phases of Russian operations. Phase one, in January 2022, focused on strategic cyber espionage and pre-positioning; phase two, from February to April, focussed on initial destructive cyber operations and military invasion; phase three, from May to June, sought to sustain targeting and attacks (while the Ukrainian counter-offensive regained territory, especially in the northeast); phase four, from August to September, focussed on maintaining footholds for strategic advantage; and phase five, from October to December, concentrated on renewing the campaign of disruptive attacks.[150]

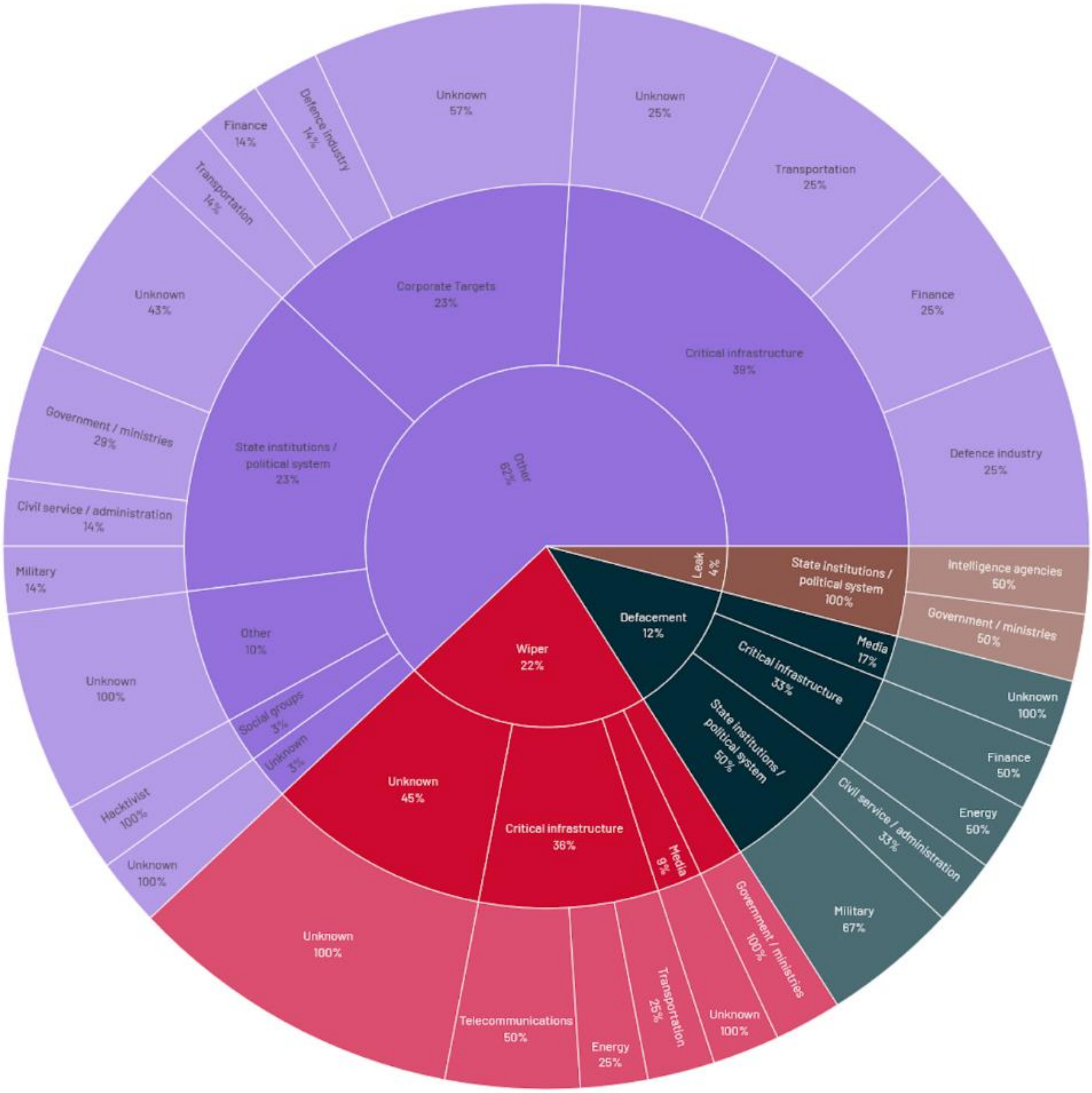
War is hardly an algebraic or algorithmic action.

To summarise the Russian cyber-attacks against Ukraine since November 2021, the following EuRepoC analysis (Figure 8) differentiates the targets from the function of the type of attacks. As the analysis clearly shows, regardless of the type of attack, the main purpose of Russian attacks has been to cripple the Ukrainian state and society. Rather than using cyber-digital means to create destructive or denying effects on military forces or weapon systems, the overall Ukrainian will and ability to defend the country was targeted. It should not be forgotten that, in parallel with the relatively low-impact cyber-attacks, the Russians continued to kill civilians and other non-combatants, to steal and destroy Ukrainian private and public property, including cultural heritage, and to destroy Ukrainian infrastructure, from kindergartens to maternity wards, roads and power plants. War is hardly an algebraic or algorithmic action, but violence tends to be taken to extremes.[151]

[150] Google, "Fog of War" (see note 138): 15. One should note that these phase-characterisations are constructed *ex post factum* by Western analysts.

[151] von Clausewitz, *Vom Kriege* (see note 3), 1:1:3.

Receivers of cyber operations attributed to Russia and targeting Ukraine since November 2021*



The graphic displays operation type and receiver category of all 27 incidents attributed to Russia and targeting Ukraine since November 2021* that EuRepoC covers | Note: * referencing the start date of the incident

Figure 8. Targets of various types of Russian cyber-attacks against Ukraine since November 2021. Data: EuRepoC. Data analysis: Jonas Hemmelskamp.

Early on, it became clear how poorly and slowly the Russian ground offensive lines managed to advance. Along the Black Sea coast, Russia succeeded in establishing a link to Crimea, illegally annexed in 2014, but the defence of Mariupol and Kyiv came to represent Ukrainian determination and ability to fight. The numerous cyberattacks activities failed in bringing down the government, the state, and the nation. In particular, the lack of strategic and military operational significance of the Russian network operations surprised many observers. As Lewis concludes, Russia has been unable to achieve any political effect by disrupting finance, energy, transportation, and government services to overwhelm defenders' decision-making and create social unrest on a meaningful scale. Four months of war led him (refreshingly) to note that "Cyberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict."[152]

Recalling how cyber sabotage was thought to stop trains, divert them to false destinations, or cause them to collide, the Russian inability to destroy Ukrainian rail transportation even by traditional military means puts both the limits of cyber capabilities and Russian weakness into perspective. The fact that some Belarussian "cyber partisans" most likely managed to sabotage some rail traffic signifies more about the co-existence of careful preparation, even insider information, and weak cybersecurity than it does about the utility of "cyber weapons" in war.[153]

Explaining Ukrainian survival

If Ukraine was seen by the Russians as a cyber range to gather intelligence and test attack methods, Russian malicious and harmful cyber activities in the 2010s forced the Ukrainians to take resilience, cybersecurity, and cyber defence seriously. In this endeavour, Ukraine received considerable financial, material, and intellectual support from Western governments and cybersecurity companies. Resources have been directed towards the development of legislation, policies and strategies, units and organisational capacity, and the skills and competencies of the workforce.[154] Indeed, the director of the U.S. National Security Agency's Cybersecurity Directorate, Rob Joyce, praised the detailed cyber intelligence provided by the private sector in support of Ukraine's cyber defence and resilience.[155]

[152] James Lewis, *Cyber War and Ukraine.* Center for Strategic and International Studies. (June 2022): 1–3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash (accessed 14 March 2023). Lewis also notes how militarily insignificant private sector attacks against Russian websites have been. See, also Mika Kerttunen, "Cyber War from Science Fiction to Reality", *Sicherheit und Frieden*, 36:1, (2018): 27–33, DOI: 10.5771/0175-274X-2018-1-27; and Ciaran Martin, "Cyber Realism in a Time of War", Blogpost, *Lawfare,* 2 March 2022, https://www.lawfareblog.com/cyber-realism-time-war# (accessed 14 March 2023).

[153] Voice of Belarus, "Cyber Partisans", 2023, https://www.voiceofbelarus.org/tag/cyber-partisans/ (accessed 14 March 2023).

[154] Bateman, "Russian Invasion" (see note 144); Nick Beecroft, "What the Russian Invasion Reveals About the Future of Cyber Warfare", Carnegie Endowment for International Peace (19 December 2022), https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 (accessed 14 March 2023); Soldatov and Borogan, *Russian Cyberwarfare*, (see note 100): 4; and Jason Healey, "Ukrainian Cyber War Confirms the Lesson: Cyber Power Requires Soft Power", *Council on Foreign Relations,* 4 April 2023, https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power, (accessed 17 April 2023).

[155] Cate Burgan, "Lessons From Ukraine: NSA Cyber Chief Lauds Industry Intel", *MeriTalk,*19 October 2022, https://www.meritalk.com/articles/lessons-from-ukraine-nsa-cyber-chief-lauds-industry-intel/, (accessed 14 March 2023)

The attack on Ukrainian satellite communications[156] provides a good example of the interaction between cyber-digital and physical-manoeuvre warfare, tactical actions and strategic impact, the absolute and the real, and the duellists. The Russian cyberattack on Viasat/KA-SAT 9A broadband internet service was clearly intended to isolate the Ukrainian government from its external and internal audiences and to disrupt and limit its situational awareness, decision-making, and command-and-control as a five-prong ground offensive was launched against the country. The attack, while successful in itself, was of no further operational or strategic benefit, as the Ukrainian government was able to restore and maintain electronic communications.

President Zelensky's self-shot video posting, "*Tut*", meaning "We are all here",[157] on the evening of 25 February became one of the most powerful information operations in history. In 37 seconds, the world realised that the Russians had not succeeded, that the battle had only just begun. The next day, Ukraine demonstrated a whole new way of e-government when Ukraine's Vice Prime Minister and Minister of Digital Transformation, Mykhailo Fedorov, tweeted for help from Elon Musk,[158] followed by a spree of other requests to various non-state actors. PayPal, Visa, Mastercard, SAP, Oracle, Netflix, and YouTube were among other corporations that responded to Fedorov's tweets and suspended or disabled services in Russia.[159]

At the request of the Ukrainian government, Elon Musk's Space Exploration Technologies Corporation (SpaceX) reinstated Ukraine's internet connectivity. Commentators have framed the legal nature (and consequences) of SpaceX's delivery as a contribution to the war effort.[160] Russia has accused SpaceX of "supplying the fascist forces in Ukraine with military communication equipment."[161] Military observers note that Starlink can "interact with UAVs and, using big data and facial recognition technology, might have already played a part in Ukraine's military operations against Russia."[162]

The Ukrainian government's countermove to replace one satellite communications channel with another allowed the government and military leadership to continue to command and communicate via satellite. The significance of the Viasat attack, however, needs to be assessed against the totality of Russian and Ukrainian dependencies, objectives, and activities at the end of February 2022. Rather than being perceived as the main Russian cyber-

[156] See, for example, Arielle Waldman, "Viasat confirms cyber attack on Ukraine customers", *TechTarget* (30 March 2022), https://www.techtarget.com/searchsecurity/news/252515351/Viasat-confirms-cyber-attack-on-Ukraine-customers (accessed 14 March 2023); Sam Cohen, "AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat", *Just Security*, 12 September 2022, https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat/ (accessed 14 March 2023); and Cyber Peace Institute, "Case Study Viasat", June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (accessed 14 March 2023).

[157] "Volodymyr Zelensky takes to the streets to rally people against Russian invaders", *The Telegraph,* 25 February 2022, https://www.youtube.com/watch?v=0En27IsHaL0 (accessed 14 March 2023).

[158] Mikhailo Fedorov (@FedorovMykhailo), *Twitter*, 26 February 2022, 2:06 AM, https://twitter.com/fedorovmykhailo/status/1497543633293266944?lang=en (accessed 14 March 2023).

[159] Sarah Roach, "Ukraine wants tech companies to sever ties with Russia. Here's how they're responding", *PROTOCOL,* 7 March 2022, https://www.protocol.com/bulletins/ukraine-fedorov-big-tech, (accessed 14 March 2023).

[160] Kartik Bommakanti, *Starlink and Ukrainian Military Performance: Implications for India: How Has Elon Musk's Starlink Network Played An Important Role In Strengthening The Ukrainian Military's Might?,* 2 June 2022, https://www.orfonline.org/expert-speak/starlink-and-ukrainian-military-performance/ (accessed 14 March 2023).

[161] Elon Musk (@elonmusk), *Twitter*, 9 May 2022, 3:40 AM, https://twitter.com/elonmusk/status/1523462998081572864 (accessed 14 March 2023).

[162] Tanmay Kadam, "China 'Deeply Alarmed' By SpaceX's Starlink Capabilities That Is Helping U.S. Military Achieve Total Space Dominance", *The EurAsian Times,* 9 May 2022, https://eurasiantimes.com/china-deeply-alarmed-by-spacexs-starlink-capabilities-usa/ (accessed 14 March 2023).

kinetic, command-and-control warfare (C2W), or information warfare vector, the Viasat attack may have been a supportive one, attempting to force the Ukrainian leadership to rely more on terrestrial (radio and landline) communications. As long as the Russian operational concept remains classified, contemporary assessments of the success and significance of the Viasat attack will be limited.

The U.S. Cyber Command highlights its "Defend Forward" strategy and the Hunt Forward Operations conducted by a joint U.S. Navy and U.S. Marine Corps team of the Cyber National Mission Force from December 2021 to March 2022, "before the invasion." The Cyber Command explains that, in addition to Hunt Forward Operations on the ground, the team had provided remote analytic and advisory support, and it also conducted network defence activities aligned to critical networks.[163]

Microsoft's analysis offers three rather Microsoft-centric technological explanations for the limited operational impact of the Russian information warfare. First, Ukrainian digital operations and data assets have been dispersed and distributed across borders and into the public cloud. Second, advances in cyber threat intelligence, including the use of artificial intelligence, have helped make it possible to detect Russian attacks more effectively. Here, Microsoft played a role in writing a code to counter a FoxBlade data wiper, sharing the code with the Ukrainian government, and, as suggested by the U.S. Deputy National Advisor for Cyber and Emerging Technologies, Ann Neuberger, shared the information and the code with other European governments.[164] Third, internet-connected endpoint protection has made it possible to rapidly distribute protective software code quickly to both cloud services and other connected computing devices to identify and disable the malware in question.[165]

Lewis credits Ukrainian (cyber) defences for the very limited effect of Russian cyber-attacks. For example, even when employing eight different families of destructive software targeting Ukrainian government websites, energy and telecom service providers, financial institutions, and media outlets, "the full suite of Russian cyber capabilities" failed, he argues. Importantly for the purposes of this study, he raises the questions about the balance between defence and offence in cyberspace, the utility of offensive cyber operations, and the requirements for planning and coordination.[166]

Wilde explains the unmet (Russian and international) expectations by claiming that the operational command and capabilities (units) of Russia's Information Operations Troops (Voyska Informatsionnykh Operatsiy) are accustomed and focused on intelligence, subversion and other political goals, rather than combined-arms warfare in direct support of military operations. In addition to the politically-oriented security and intelligence agencies, Russian practice may reflect their broader conceptual thinking about the utility and

[163] U.S. Cyber Command, "Before the Invasion: Hunt Forward Operations in Ukraine", 28 November 2022, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/, (accessed 17 April 2023); U.S. Cyber Command, "'Committed Partners in Cyberspace': Following cyberattack, US conducts first defensive Hunt Operation in Albania", 23 March 2023 https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/, (accessed 17 April 2023).

[164] Susan Landau, "Cyberwar in Ukraine: What You See Is Not What's Really There", Blogpost, *Lawfare,* 30 September 2022, https://www.lawfareblog.com/cyberwar-ukraine-what-you-see-not-whats-really-there (accessed 14 March 2022).

[165] Microsoft, *Defending Ukraine* (see note 148): 2, 5; and The German Marshall Fund, "The Foreign Policy of Technology, with Ambassador Nate Fick", Webinar, 2 February 2023, https://www.gmfus.org/event/foreign-policy-technology-ambassador-nate-fick (accessed 14 March 2022).

[166] James Lewis, *Cyber War and Ukraine,* Center for Strategic and International Studies (June 2022): 1–3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash (accessed 14 March 2023).

exploitation of the information environment.[167] Incompetent defence planning, including intelligence, perhaps filled with wishful thinking and operatives serving superiors with assessments they are expected to hear and like, may have created a false sense of awareness and confidence among Russian decision-makers.

Chris Kreps reminds us that the war is not over yet. He argues that the Kremlin may have excluded the Russian security services' cyber personnel from battle-planning, and that thorough cyber operations planning never materialised. He also suggested (in mid-March 2022) that Moscow would have wanted to keep Ukrainian networks operational for its own use. He warns that if and when Russia's political and operational situation deteriorates, it could lead to devastating Russian retaliation against targets deeper in the West.[168]

The war has clearly intensified the digitalisation, or informationisation, of the battlefield. Drones have emerged as important platforms of intelligence gathering. Similarly, private companies, from global giants such as the aforementioned SpaceX or Microsoft to start-ups like the synthetic aperture radar company Iceye, which provides satellite imagery,[169] signify the out- and crowdsourcing of certain aspects of warfare. The way in which smartphones and other connected technologies can reduce operational security and enable communication even in all-out war should come as no surprise.

The ability to have accurate national, operational, and tactical situational awareness is an essential virtue and feature of warfare, whether cyber or non-cyber. In addition to Ukrainian and Western intelligence capabilities, private citizens and non-Ukrainian entities began gathering digital information from telecommunication and internet traffic, including social media postings, in an unprecedented manner. It is too early to assess the strategic or operational impact that such privatised and open-source intelligence has had, but some Ukrainian strikes are said to have been based off such information. [170]

Despite all the cyber-digital efforts and success stories, the war in Ukraine once again seems to have become another "cyber war that wasn't."[171] One misleading benchmark was the admittedly cunning way in which the Kremlin managed to seize Crimea and the regions of Donetsk and Luhansk regions in 2014. In 2022, such Russian creativity was missing, and Ukraine was better prepared to respond to Russian conventional military and cyberspace attacks.[172]

Russia's meagre cyber success has surprised those who had become believers of "Cyber Pearl Harbor" or "Cyber 9/11" and who inflated the notions of war and warfare. The less-than-expected, even poor, Russian performance on the cyber front call into question the value of testimony such as that of General Nakasone before the U.S. Senate Armed Services Committee in 2018, which portrayed Russia as a full-scope cyber actor with sophisticated tactics, techniques, and procedures for cyber operations, "likely to continue to integrate

[167] Gavin Wilde, *Cyber Operations in Ukraine: Russia's Unmet Expectations*. Carnegie Endowment for International Peace (December 2022).

[168] Chris Krebs, "The cyber warfare predicted in Ukraine may be yet to come", *Financial Times*, 20 March 2022, https://www.ft.com/content/2938a3cd-1825-4013-8219-4ee6342e20ca (accessed 14 March 2023).

[169] Iceye.com.

[170] "Mobile phone data leads Ukraine to Russian barracks", *The Telegraph,* 3 January 2023, https://www.telegraph.co.uk/world-news/2023/01/02/ukraine-russia-war-updates-live-ukraine-russia-war-drones-strike/ (accessed 14 March 2022).

[171] Wilde, *Cyber Operations* (see note 171). The expression of cyber war that wasn't refers to Martin Libicki's 2015 chapter "The Cyber War that Wasn't" (in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers [Tallinn: NATO CCDCOE, 2015]: 49–54).

[172] The Russian five-prong ground offensive in late February and early March 2022 and the concentration of force in time instead of place, had it succeeded, would most likely have been regarded as creative. The thrust vectors for various reasons reached their points of culmination well before the Russian geographical or functional objectives.

cyber warfare into its military structure to keep pace with U.S. cyber efforts."[173] In a March 2023 testimony, General Nakasone assessed "Russia's military and intelligence cyber forces" as "skilled and persistent." After 54 weeks of warfare in Ukraine, he noted that Russia had "attempted to influence elections, through malign activities, in the United States and Europe and has enabled intelligence collection on a global scale" and launched an "indiscriminate cyberattack on Viasat satellite communications in Ukraine and across Europe in support of the invasion of Ukraine last year."[174]

Compared to the US, the scope of Russian military cyber competence is focussed and mixed. In addition to network operations conducted by civilian agencies such as the Central Intelligence Agency and the National Security Agency, the Department of Defense is developing military cyber capabilities to support military operations, including combat. In Russia, both civilian and military agencies focus on supporting the federal state rather than combat forces. Russian state network competence is formidable not because of its combat effectiveness, but because of its orientation and composure, including proxies and non-state actors, such as criminal actors. Russian capabilities in electronic warfare and information operations further amplify the effects of information warfare.

Of course, both Russian and Chinese battlefield cyber capabilities may be a slow train coming. For the time being, however, the imperative to develop national and military cyber capabilities appears to be more communist-oppressive than combat-operational for these authoritarian regimes and, most likely, for the governments of many developing countries as well.

[173] Senate Armed Services Committee, "Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service", LTG Nakasone answered to a question on Russian cyber capabilities, 1 March 2018, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf (accessed 14 March 2023).

[174] Senate Armed Services Committee, "Posture Statement of General Paul M. Nakasone, Commander United States Cyber Command before the 118th Congress Senate Committee on Armed Services", 7 March 2023, https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf (accessed 14 March 2023).

Conclusion. *Pointillism*

The employment of cyber capabilities, military or not, by armed forces or civilian state agencies, can constitute war.

State projection of payloads that cause destructive effects in another sovereign state can be considered as violent. Whether such conceptually-constituted destruction is empirically considered to constitute a use of force or an act of war is ultimately not a legal or scientific determination, but a political one. It is of the utmost importance to understand that, while the employment of cyber capabilities is unlikely to quantitatively meet the thresholds of use of force and armed attack, it does qualitatively meet the criteria of violence and war.

The state practice of waging war and applying the methods and means of warfare to impose its political will upon other states has not disappeared. It is therefore essential to recognise the employment of cyber-digital capabilities as a use of force. This fundamentally qualitative move, an interpretation, would obligate the operating countries' politicians to restrict the means and methods of such use of force and uphold the rights of those human beings and states directly or indirectly affected by the hostilities.

Table 4 below concludes how violence, political intentionality, and the management of chance manifest themselves in the employment of cyber capabilities.

Violence, political intentionality, and the management of chance operationalised		Manifestation of violence, political intentionality, and the management of chance in the employment of cyber capabilities
Violence with the elements of hatred and animosity	Destruction of property Injury Loss of life Threatening and terrorising One-Other differentiation Accusation Demonising	Destruction of data and i.a., critical infrastructure Causing injury or loss of life through cyber-physical effects Loss of value, continuity of operations and functionality, and reputation Targeting and terrorising enabled by digitally-cumulated and synthesised information Alienation and demonising through, e.g., cyber-enabled information operations Promotion of propaganda in and through cyberspace, e.g., digitalised devices and services Incitement Foreign digital and informational interference to manipulate and polarise public opinion, influence decision-making, and erode social and societal cohesion
Political intentionality	Political subordination Adherence to the set objectives	State agency or control Adherence to the political objectives of a person or a group of political significance
Management of chance	Organisation Governance system Planning Sustainability Payload optimising	Cyber-specific structures and units Guidance and legitimising documentation such as policy, strategy, or doctrine Internal or external synchronisation with other forms of power projection, e.g., diplomacy, pressure, deception, and information operations Research and development, testing, live fire proofs

Table 4. The manifestation of violence and intentionality in the employment of cyber capabilities. Author's compilation. Sources: Carl von Clausewitz, *Vom Kriege* (Cologne: Ferd. Dümmler Verlag, 1832/1991), Buch 1:1:24, and 1:1:2, respectively; Carl Schmitt, *The Concept of the Political* (Chicago: Chicago University Press, 1932); Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017); United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/70/174 (22 July 2015).

In analysing the manifestation of the tendencies of war in cyber activities, one should focus not on agency, but rather on the acts themselves. In the light of the Russo-Ukrainian War, the privatisation of war has only increased. It is not only the private contractors familiar from the Western Balkans, Iraq, and Afghanistan who are operating on the battlefield, but also private citizens and essentially civilian companies who are now attempting to try to influence the outcome of hostilities, virtually and at a distance. Similarly, the established means of potentially violent and hostile state power projection, the actual situation on the ground, and the effects created and methods used must be taken into account in political and legal determinations.

In particular, the more truthful we find the contemporary expanded, hybrid, and participatory descriptions of war, the less weight we should place on the established, striated interpretations of war. It should be noted, however, that the established forms and appearances of war and warfare have not necessarily disappeared. It is as dangerous to believe in radical change as it is to believe in cemented continuity in war.

Military cyber capabilities are primarily employed for espionage, oppression, subversion, and destabilisation.

As long as military cyber capabilities are being developed for military operational purposes but without doctrinal clarity or quantitative and qualitative investment in workforce development, progress will remain meagre in most armed forces. Kinetic militarily-significant effects are still far easier and more effective projections of political power. If death, destruction, and black smoke are deemed necessary, cyber is not the choice.

In the light of Russian war against Ukraine in 2022, cyber-attacks, military or otherwise, do not appear to be capable of creating political or strategic effects in armed conflict.

Once again, we need to be reminded of Clausewitzian warnings that war is a play of chance between probability and improbability, the play of friction in human and technical affairs, and that reality is always less than the absolute. The employment of cyber capabilities does not seem to create the broader, long-term, decisive effects that military campaigns and war proper aim to achieve. The issue is not one of death and destruction, but rather of the scale of such violent and destructive effects that the employment of cyber capabilities can also create. Moreover, even effective cyber-attacks against civilian and societal infrastructure and services do not easily contribute to operational or tactical military success. It is not as easy, cheap, or fast as has been advertised.

As noted above, the play of probability/improbability and chance is as omnipresent a feature of life as it is an element of war. It is clear that the conduct of malicious cyber activities remains suboptimal as that of any human affairs. The military operational utility of cyber operations has been exaggerated. Cyber operations cannot be prepared, planned, or implemented at the speed of light. Similarly, infantry does not advance at the speed of bullets and air operations are not conducted at Mach 1. Furthermore, while it is possible to calculate the first-order effects of a network attack, the n^{th} order effects, such as operational, strategic, political, and moral effects, remain best guesses. It is too tempting not to recall of the notion of friction, which is also present in digital and computer-based activities.

Russian prowess for destructive and denying cyber operations, cyber espionage, and information and influence operations has not vanished. The capabilities primarily designed for non-military purposes of societal control, oppression, subversion, and sabotage have proven to be suboptimal for supporting conventional military operations. Russian strategic and tactical electronic warfare, however, seems to remain effective.

Cyber defence appears to be stronger than cyber offence.

Wars shape our thinking about war. The interventionist wars of 1990–1991, 1999, and 2003 created an ideal, even objective illusion,[175] of informationised warfare, first by digitalisation of the battlefield - that is, military communications and information flows - and later by making information itself a payload, a "weapon" as many would like to claim. Information has been long been a target. Perhaps the Ukrainian campaign/war teaches us that cyber defence prevails over cyber offence. Two intertwined factors, one quantitative, the other qualitative, justify the assertion. To maintain the momentum of a cyber operation or campaign in a target-specific environment, requiring target-specific intelligence and payloads, the attacker needs a higher volume and rate of production than the defender. Stockpiling malware will not do much to solve the sustainability problem, as software vulnerabilities may be fixed or software may be changed. Unlike the enduring war horses like the Lee-Enfield m/1895 or the AK-47, malware has a much shorter shelf life.

Although the raison d'être of cyber operations can be found in the improved precision of targeting and fire, the ideals of manoeuvre warfare and the *ex post facto* anchoring of Sun Tzu's illusionist imperative to win a war without fighting, the reality of the Russo-Ukrainian War demonstrates that the employment of cyber capabilities has become merely a tool in a war of attrition. The virtual bombardment of Ukrainian systems parallels the continued shelling of Ukrainian cities, infrastructure, and defences. It is as if the Russians are attempting to apply John Warden's theory of airpower to cyber-conventional warfare, involving leadership, processes, infrastructure, population, and fielded forces, but besides death and destruction, with no operational or strategic return on military or political investment.[176]

Rehabilitate Command-and-Control Warfare (C2W).

It is time to recontextualise network operations. Although painful for all domain enthusiasts, cyber-digital network operations can find a suitable home within the operational concept of command-and-control warfare (C2W). The benefits of repositioning computer network operations include the creation of synergies between currently-blurred network, information, and psychological operations, electronic warfare, and the physical destruction of C2 systems and services. In light of the Russo-Ukrainian War, cyberspace operations alone do not create sufficient effects to support military manoeuvres. On the contrary, the lessons learned from the war, the way the Chinese approach information warfare, and the branches and functions under the U.S. Army Cyber Command – and some national commands as well – support a rethinking of the doctrinal foundations and organisational home of network operations. Such a move would also bring needed clarity between military effect-creating operations, (civilian) security and intelligence services' effect-creating operations, and intelligence/espionage operations. The conclusion of the 1996 US joint doctrine on C2W sounds both accurate and relevant:

[175] Epistemic implications of positional dependence of observations and observation-based reflections (Amartya Sen, *At Home in the World* [New York: Liveright Publishing Corporation, 2022]: 216–217).

[176] John A. Warden, "Strategy and Airpower", *Air & Space Power Journal.* Vol 25:1 (2011): 66–78.

> *“Command and control warfare is a warfighting application of Information Warfare in military operations and employs various techniques and technologies to attack or protect command and control. C2W is the integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence. C2W should be an integral part of all joint military operations and requires extensive planning and coordination to ensure that C2W operations are fully integrated with other portions of operation and plans. Detailed planning, training and exercises, and understanding of multinational operations allow for successful applications of C2W.”*[177]

“Cyber” as a prefix implies much more than a digital layer. As an area of operations, alternatively: cyberspace, cyber domain, or information environment, it is too important and sensitive to be siloed. As US and Estonian practises show, cyberspace operations are more than code-based network operations; the same military authorities direct electromagnetic spectrum and information operations. A coherent doctrine is more useful a step to unify efforts and amplify effects than a nominal cyber domain or a command. A revitalised command-and-control warfare doctrine would give meaning to the empty and awkward notion of hybrid warfare – and help move away from it.

We cannot assume that the meagre Russian military operational success in and through the Ukrainian cyberspace will entail increased security and stability of the global cyberspace.

The lessons learned from the war may direct efforts to continue effect-creating, destabilising, and criminal cyber-attacks, especially in peacetime. It is also likely that we will hear apologies in defence of utopia: that the Ukrainian war is *sui generis,* that the next war will be different, and then we may witness military cyber success. This is the interplay between the enduring elements and the changing nature and characteristics of war. It is this uncertainty, together with the aspirations of the cyber-industrial complex, that will continue to keep the development of military cyber capabilities on the agenda.

Politically and doctrinally, we need to exercise caution when predicting future outcomes.

Analysis of the events in Ukraine highlights not only the confusion in the use of the terms of war and warfare, but also between the undefined terms of cybersecurity, resilience, and defence. Is the problem in the development and use of information and communication technologies inherently a security, resilience, or defence one? Defining and demarcating problems in one way tends to provide the solution in the very same way. We stand where we sit.

Private and organisational desired end-states should not condition professional appraisals. Political colouring is the privilege of politicians. Instead, experts should exercise and demand conceptual clarity and epistemological, ontological, and methodological rigour in their assessments. It all starts at home.

[177] Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare (C2W)* (7 February 1996).

Cyber isn't a *Wunderwaffe.* The difficulty, slowness, and ineffectiveness of the employment of cyber capabilities in war should keep the threshold to wage war high. The relative ease of employing cyber capabilities for peacetime espionage and "grey zone" subversion should remind us not only of the need for resilience and cybersecurity, but also of the importance of conflict prevention. We should not celebrate cyber operations as a harmless expeditionary, fleet-in-being-type of enterprise, imposing an ideal way of affairs. Political opportunism easily translates into strategic flaunty. Cyber adventurism poisons relations and tends to escalate tensions. Accordingly, an increase in espionage and destructive attacks should warn us of a risk of war, as should as troop concentrations, close-proximity offensive exercises, and frequent airspace violations.

Public scrutiny is needed.

As it is temptingly easy and sufficiently-effective to conduct peacetime network espionage, data theft, and date destruction operations, parliaments, people, and the press should critically question national and governmental motives for developing national or military cyber capabilities. In some countries, cyber commands and other cyber units may be developed for domestic political purposes.

A tool unfit to make war can make a war through peacetime operations.

The war in Ukraine signifies the rise and growing impact of public-private partnerships. Public caution and scrutiny are needed when voluntary military units, private sector companies, and private citizens begin to engage in cyber-digital exchanges outside the controlled, accountable use of force, or further, when they offer their perhaps even well-meaning services for hire.[178]

Parliaments, people, and the press should therefore demand a clearer separation of powers and mandates. This can be achieved by deliberately separating, rather than centralising, state cyber powers: national incident management, law enforcement, intelligence, military cyber defence, and diplomacy. The second step required is a deliberate and constitutional involvement of legislatures and the public/private sectors in cyber-related preparation and decision-making.[179] War, operations, and violence as not only continuation of politics but elements of politics are appropriate, relevant, or adequate for very few political problems. Cyber capabilities, like any other form of violence, necessitate guarding the guardians.

[178] On surveillance-for-hire, see e.g., Meta, "Threat Report on the Surveillance-for-Hire Industry", 15 December 2022, https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf (accessed 14 March 2023) and "Meta Policy Recommendations for Tackling the Surveillance-for-Hire Industry", 15 December 2022, https://about.fb.com/wp-content/uploads/2022/12/Meta-Policy-Recommendations-for-Tackling-the-Surveillance-for-Hire-Industry.pdf (accessed 14 March 2023).

[179] Mika Kerttunen, "Rule of law in cyberspace", Blogpost. *Directions.* EU Cyber Direct, 11 October 2021, https://directionsblog.eu/montesquieu-for-cyberspace/ (accessed 14 March 2023). On the broad literature on constitutionalism, see, for example, Martti Koskenniemi, "Constitutionalism as Mindset: Reflections on Kantian Themes About International Law and Globalization", *Theoretical Inquiries in Law,* 8:9 (2006): 9–36; and Kaarlo Tuori, "European constitutionalism", in *The Cambridge Companion to Comparative Constitutional Law,* ed. R. Masterman and R. Schütze (Cambridge: Cambridge University Press, 2019): 521–553, https://helda.helsinki.fi/bitstream/handle/10138/312573/european_constitutionalism_2.pdf?sequence=1 (accessed 14 March 2023).

Abbreviations

APT	Advanced Persistent Threats
C2	Command-and-Control
C2W	Command-and-Control Warfare
CCCS	Canadian Centre for Cyber Security
CN	Canada
CNMF	Cyber National Mission Force
DE	Deutschland (Germany)
DOD	Department of Defense
ECT	Expeditionary Cyber Teams
EE	Estonia
FSB	Federal Security Service of the Russian Federation
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICT	Information and communications technology
KA-SAT	Ka-band satellite
MaCI	Major Cyber Incidents
MCU	Military Cyber Units
NMS-CO	The National Military Strategy for Cyberspace Operations
OECD	Organization of Economic Cooperation and Development
PLA	People’s Liberation Army
RU	Russia
SSF	Strategic Support Force
SVR	Foreign Intelligence Service of the Russian Federation
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
US	United States

Acknowledgements

This research would not have been possible without the generous intellectual support of the EuRepoC consortium community. Sebastian Harnisch, Kerstin Zettl-Schabath, Kim Schuck, and Linda Liang from the University of Heidelberg; Annegret Bendiek, Matthias Schulze, Camille Borrett, Jakob Bund, Emma Plate, and Jonas Hemmelskamp from the Stiftung Wissenschaft und Politik; Matthias Kettemann and Martin Müller from the University of Innsbruck; and Eneken Tikk from the Cyber Policy Institute have all helped, guided, and corrected me along the way. Callahan Shelley's skilful editing was a great help to my argumentation. The German Federal Foreign Office, particularly Ambassador Regine Grienberger, was instrumental in providing much-appreciated financial support for the project. Marion Calistri (SWP) and Susanne Geiselhart (UoH) showed that German bureaucracy can be effective, flexible, and friendly.

Mika Kerttunen is Adjunct Professor Military Strategy Finnish National Defence University, Board Member Swedish Defence University and Member of The Swedish Royal Academy of War Sciences.

This Working Paper reflects the author's views.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org