ITSS
International Team
For the Study of Security
Verona

MILITARISING THE CYBERSPACE:
Offensive Cyber Capabilities Against Traditional Means

by Annalisa Guarise

ITSS Verona Magazine, Vol. 1, n. 2

Fall/Winter 2022

MILITARISING THE CYBERSPACE: Offensive Cyber Capabilities Against Traditional Means

Annalisa Guarise

To cite this article: Annalisa Guarise, *MILITARISING THE CYBERSPACE: Offensive Cyber Capabilities Against Traditional Means*, ITSS Verona Magazine, Vol. 1, no. 2, Fall/Winter 2022.

Keywords: Cyber Warfare, Offensive Cyber Operations, Non-Physical Violence, Operation Orchard, Attribution

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: December 30th, 2022

Abstract: The acknowledgment of the interconnection between the military sphere and the cyberspace domain has paved the way for the development of new states' capabilities. This paper explores how cyberspace lends itself to *offensive* military operations, comparing these emerging military cyber capacities to traditional weaponry. Cyberspace's ever-evolving and elusive nature differs deeply from the traditional operational fields: an entirely man-made domain but, paradoxically, harder to control and delineate. On the other hand, offensive cyber operations (OCOs) do aim at gaining the same strategic advantages of traditional combat. But are their effects and goals only strategically similar to conventional warfare's ones, or do they inflict the same level of violence as well? Only the adoption of a broader definition of "violence" allows the recognition of the harm caused by these new war means, helping to build structures to counter them, and leading national actors to bear responsibility for their actions. For the time being, relevant examples of OCOs are limited to the strategic and operational levels of war, while from a tactical perspective the combination of cyber capabilities with traditional forces is still not well developed. This scarcity of cases might also derive from a difficulty in attributing a cyber-attack to a specific state actor. In fact, cyberspace's nature exacerbates the timeless issues of attribution under international law, increasing the importance of data gathering by cyber-security firms and intelligence agencies to identify those responsible for cyber-attacks.

The relatively new domain of cyberspace has posed unprecedented threats as well as incredible opportunities. States' military capacity has been able to gear up for the former and to develop new mechanisms to exploit the latter.

This paper explores how cyberspace lends itself to *offensive* military purposes, deepening the analysis of the substructures that enable such fitting. More in detail, the aim is to compare the traditional weaponry and the new military cyber potentialities, investigating the differences between their violent nature and their concrete application to the three confrontational levels – strategic, operational and tactical.

The first two sections of this work aim at providing the conceptual and theoretical framework to the core elements on which the further analysis builds. First of all, the opening section will trace a comprehensive definition of cyberspace, considering it as the broader domain under which the military capabilities analysis will take place. The interconnection between the cyber and the military field will highlight some fundamental peculiarities of the virtual realm. Following, the second section will address the *offensive* cyber capabilities of states by framing their characteristics and the elements that ensure their concrete deployment.

The last two sections focus instead on the comparison between the *kinetic* military domain and the cyber realm. More in detail, the third one will evaluate the notion of violence, as it constitutes a fundamental parameter in assessing potential differences between physical and cyber offensive operations. Finally, the fourth section will instead present empirical examples of the application of cyber operations to the three well-known levels of war, namely the strategic, operational and tactical ones. Following, conclusions are offered.

Conceptual Framework

The Cyberspace Domain

As of today, there is still no univocal definition for the concept of cyberspace.[1] In a widely cited work, Daniel Kuehl combines different perspectives in elaborating the definition of cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".[2] This definition results particularly comprehensive as it encompasses the operational and unlimited nature of the cyberspace; its relations to the information domain as cyberspace is used to act on information; both the physical and technological nature of it, especially explaining its functioning, i.e. through electromagnetic activities and interconnected networks based on specific technologies. Ronald J. Deibert and Rafal Rohozinski widen the understanding of cyberspace, underlying how it is nowadays an indispensable component of political, social, economic and military power worldwide.[3] Deepening the latter aspect of this consideration, the U.S. Department of Defence has started to consider cyberspace as the fifth domain of military operations, alongside with the kinetic and physical domains of land, sea, air and space.[4]

The acknowledgment of the interconnection between the military sphere and the cyberspace domain furthers the reflections. The cyber realm is in fact unique and deeply different in nature from the traditional operational fields, as this domain is entirely man-made but, paradoxically,

[1] Tomasz Zdzikot, "Cyberspace and Cybersecurity", in *Cybersecurity in Poland*. Springer, Cham (2022): pp 9-21, https://doi.org/10.1007/978-3-030-78551-2_2, 11.

[2] Daniel T. Kuehl, "*From Cyberspace to Cyberpower: Defining the Problem*", in "Cyberpower and National Security", ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (National Defense University Press, 2009): pp 1-17, https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210, 29.

[3] Ronald J. Deibert, and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (March 2010): pp. 15-32, https://doi.org/10.1111/j.1749-5687.2009.00088.x, 16.

[4] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, Washington, D.C., U.S.A., 2011: 1-13, https://www.defense.gov/news/d20110714cyber.pdf, 5.

harder to control and delineate. The very nature of the cyber domain leads thus to two fundamental consequences. First, since cyberspace is continuously evolving thanks to the infinite multiplicity of actors that spontaneously contribute to its ongoing and never-ending building, any attempt to draw a map of the Internet will be outdated before it is even completed.[5] Secondly, the transnational nature of such a domain renders it increasingly problematic to govern, because it implies the lack of a central authority as well as the struggle in distinguishing between military and civil actors. Consequently, the fast-changing geography of the internet and its spontaneous amplification, along with the – lack of – transnational governance render this domain a fertile ground for new forms of military confrontation.[6]

These specificities have led to the identification of three main types of military operations that can be carried out through a computer: (a) *defensive* cyber operations, i.e. actions aiming at protecting or monitoring unauthorised activities within a government information system; (b) cyber *espionage* operations, i.e. actions aiming at gathering data from target or adversary information systems and, (c) *offensive* cyber operations (OCOs), i.e. actions aiming to disrupt, deny, degrade, or destroy information resident in computers and computer networks.[7] The next section focuses on the latter.

Offensive Cyber Capabilities: Characteristics and Functioning

The militarization of the cyber realm brings new operational possibilities to the state: its Offensive Cyber Capabilities (OCCs). The level of a state's OCCs is determined by the combination of several factors: Florian J. Egloff and James Shires recall that these offensive abilities consist, first of all, of technological capacities such as infrastructure for reconnaissance and control, knowledge

[5] Robert Fanelli, "Cyberspace Offense and Defense," *Journal of Information Warfare* 15, no. 2 (2016): pp. 53-65, https://www.jstor.org/stable/26487531, 54.

[6] Andrea Calderaro and Anthony J. Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building," *Third World Quarterly* 41, no. 6 (March 19, 2020): pp. 917-938, https://doi.org/10.1080/01436597.2020.1729729, 919.

[7] Aaron Brantly, and Max Smeets, "Military Operations in Cyberspace," in *Handbook of Military Sciences*, eds Anders McD Sookermany (Springer, Cham, 2020): pp 1-16, https://doi.org/10.1007/978-3-030-02866-4_19-1, 4.

about vulnerabilities, open-source and commercial tools.[8] Moreover, OCC's include the abilities individuals might possess for developing, testing, and deploying these technological capabilities.

Offensive Cyber Operations (OCOs) carried out through cyberspace require, as within the kinetic domain, specific conditions and characteristics to succeed. Herbert S. Lin performs a comprehensive analysis of the technological means that a cyber-attack requires.[9] First, it is necessary to identify a *vulnerability* for the attacker to exploit. A system's unintentional defect or weakness may be detected and thus used by adversaries that have the technological capacities to recognize it. Secondly, in order to exploit such detected vulnerability, the adversary must clearly have *access* to it. Access can be both remote or close. As for the former, the classic scenario encompasses an attack launched at some distance from the target through an access path provided by the internet, a VPN, a dial-up modem or wireless. In case of close access, the attack takes place thanks to a physical means, such as a local installation of hardware or software functionality, placed in close proximity to the targeted computer/network by non-adversaries parties. After the vulnerability has been exploited, the concept of *payload* defines the actions that the aggressor may undergo. Finally, the *effects* of the attack depend on the kind of offensive operation that has been carried out. More specifically, in the case of cyber-exploitations, the information that should be accessible only to authorised parties is instead made available for the aggressor. In the case of cyber-attacks, the malicious operation seeks to cause a loss of integrity, authenticity or availability of the targeted device.

Between Theory and Practice

Understanding OCOs' Violence

The understanding of the functioning of OCOs allows for a deeper analysis of the relationship between the newest cyber weapons and the traditional military capabilities of states. Richard J.

[8] Florian J. Egloff, and James Shires, "The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence," *European Journal of International Security*, (October 12, 2021): pp. 1-20, https://doi.org/10.1017/eis.2021.20, 3.

[9] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010): pp 63-86, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf, 65-68.

Harknett and Max Smeets propose the view that cyber campaigns may actually represent an alternative to war.[10] As they do not resort to the brutal confrontation of kinetic war, they are perceived as profoundly different from the Clawsewitzian understanding of the notion: in this new scenario, computers are used in place of conventional weaponry, making the attack seen as less bloody. On the other hand, they do aim at gaining the same strategic advantages of traditional combat.

The dilemma here is whether the effects of OCOs are only strategically similar to the ones of conventional warfare, or if they are equivalent to their infliction of violence as well.

The assessment of whether cyber weapons and cyber warfare are "less violent" than conventional warfare must begin with the understanding of what "violence" is in relation to the effects of an attack. In this regard, the dominant academic reasoning supports a narrow understanding of what is violent, linking it only to physical and eventually lethal harm, thus concluding that cyber weapons may represent a less violent evolution of conventional warfare.[11] On this line, Jeffrey Carr proposes a definition of cyberwarfare that clearly builds on this understanding of physically-intended violence: according to him, "cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood".[12] Thomas Rid confirms this view, assessing that cyber warfare still lacks an essential component of war, i.e. the large-scale physical damage and the massive violence that eventually bend the political will of the adversary.[13] When OCCs translate into concrete OCOs, those do not lead to a level of destruction comparable to traditional weaponry. Consequently, part of the strategic studies literature concludes that cyberwarfare is indeed less violent because it costs fewer lives compared to kinetic conflicts.[14]

[10] Richard J. Harknett, and Max Smeets. "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic studies* 45, no. 4 (March 4, 2020): pp. 534-567, https://doi.org/10.1080/01402390.2020.1732354, 535.

[11] John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (November 29, 2012): pp. 101-108, https://doi.org/10.1080/01402390.2012.730485, 103.

[12] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, Inc., 2012).

[13] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35.1 (2012): pp 5-32, https://doi.org/10.1080/01402390.2011.608939, 10.

[14] Tim Maurer, "The Case for Cyberwarfare," Foreign Policy, October 20, 2011, https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/.

On the other hand, other scholars have expanded the concept of violence, supporting the idea that also non-lethal or non-physical OCOs must be intended as violent. Under this premise, new elements are taken into account beyond the mere substantial harm: Tim Stevens draws the attention to the "affective implications of cyber weapons", such as feelings of insecurity or fear;[15] similarly, Egloff and Shires underline the importance of considering as violent an act *intended* to cause harm.[16] Moreover, the authors continue the analysis explaining why it is not a semantic exercise to look at the interpretation of the term "violence".[17] Overtime, many states have undertaken several OCCs and OCOs that have caused evident harm, but because of the adoption of a narrower reading of the concept, such harm was under-appreciated or not even recognized by states themselves. A broader understanding of the notion of violence helps instead building structures to counter those harms, and leads national actors to bear responsibility for their actions.

Even if they do not always trigger physical damages, the repressive uses of OCCs are intrinsically violent as they impact on people's life by causing fears or trauma. Consequently, only with the adoption of an expanded definition of violence they can be recognized as brutal and harmful too.

Empirical OCOs Applications – the Three War Levels

Traditional military theories distinguish between three levels of war: strategic, operational and tactical. The first concerns the way in which national power – cyber-capability – is programmed to be used with the aim of achieving strategic objectives, such as weakening the adversaries' ability or even the will to engage in the conflict. The operational level regards instead the planning and conduction of the campaign. Finally, tactical refers to the combat engagement on the battlefield, thus classifying as the domain that witnesses the display of conventional weapons. How does this traditional division within the military context match the novelty brought by the cyber domain?

[15] Tim Stevens, *Cyber Security and the Politics of Time*, (Cambridge University Press 2015): 2.
[16] Egloff, and Shires, "The better angels," 10.
[17] Egloff, and Shires, "The better angels," 13.

According to Matthias Schulze, there are still no glaring examples of cyber operations that can be fully classified as war according to the strategic level.[18] However, the closer example is probably the US-planned Operation Nitro Zeus, discussed below. At the operational level, a great example is provided instead by the 2007 Israeli Operation Orchard, analysed further. As confirmed by Jonathan Butts and Michael Glover, cyber operations are deployed primarily on these two levels.[19] From a tactical perspective, however, the combination of cyber capabilities with traditional forces is still not well developed. Relevant examples are thus limited to the strategic and operational levels.

Operation Nitro Zeus was conceived by the US Cyber Command as a safety plan to restore to in case Stuxnet and the diplomatic means aiming at containing the Iranian nuclear program would have failed.[20] Nitro Zeus served in fact as a reassurance to President Obama about the fact that there were alternatives to a head-on military confrontation if Iran would have pulled out of the nuclear deal. As reported by David Sanger and Mark Mazzetti, the plan aimed at disabling Iranian air defences, its communication systems and other crucial parts of its power grid.[21] John Arquilla stresses that strategic cyber-attacks generally aim at hitting the adversary in a consistent disruptive manner without the need to oppose military forces in the field, at sea or in the air.[22] In addition, such attacks may be launched anonymously or through the use of proxies, thus decreasing considerably the risk of retaliation. Operation Nitro Zeus, even if only planned and never carried out, actually respects these criteria, as it would have guaranteed a strategic advantage to the US in case the situation escalated. The operation has also been read as a pre-emptive large-scale cyber-strike

[18] Matthias Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations," *2020 12th International Conference on Cyber Conflict (CyCon)*, Vol. 1300, IEEE (2020): pp. 183-197, https://doi.org/10.23919/CyCon49761.2020.9131733, 186.

[19] Jonathan Butts, and Michael Glover, "*Developing a Tactical Environment Cyber Operations Training Program,"* McKellar Corp Virginia Beach VA (January 2015): pp 1-69, https://apps.dtic.mil/sti/pdfs/ADA624747.pdf, 2.

[20] For a detailed overview of the Stuxnet malicious worm and of the Operation Olympic Games see: Baezner, Marie, and Patrice Robin. "Stuxnet" (No. 4). *Center for Security Studies (CSS)*, ETH Zürich (October 2017). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.

[21] David Sanger, and Mark Mazzetti, "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." *New York Times,* February 16, 2016, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

[22] John Arquilla, "The Rise of Strategic Cyberwar?," ACM, September 25, 2017, https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext.

option.[23] This perspective brings about another observation related to the strategic potential of cyber warfare: according to Nadiya Kostyuk and Yuri M. Zhukov, cyber-attacks tend to be more effective when they are not expected, thus creating a surprise effect.[24] Consequently, they result to be most valuable especially in the early stages of a confrontation.

The 2007 Operation Orchard (or Operation Outside the Box) consisted in an airstrike launched by Israel on Syrian territory, targeting a suspected nuclear reactor with military purpose in the Deir ez-Zor region. In order to mislead Syrian air-defences, Israel deployed an electronic tool able to provide false sky-picture, which tricked the Syrian radars for the whole-time span of the operation. The believed implicated technology is known as "Senior Suter": the Suter exploited the vulnerabilities and attacked the functioning of the air defence system by beaming electronic impulses into the antennas and introducing specifically customised signals. The air defence system was then corrupted by inserting misleading data with the aim to deceive.[25] Beyond the cyber domain, operational attacks tend to target infrastructures, tactical bases, tanks or ships, in order to obtain a significant advantage. In this empirical case, the use of cyber weapons in the context of the operation have enabled the kinetic attack – i.e. the bombing of the facility.

As reported by Schulze, one explanation for the scarcity of tactical cyber operations may be that they are subjected to several restrictions.[26] For example, many states that are equipped with cyber capacities decide and deploy their offensive capabilities at the higher point of the chain of command, i.e. at the strategic level. Moreover, tactical cyber operations result to be much longer than physical tactical operations in their planning and development time.

In addition, both the lack of concrete tactical examples and the scarcity of cases related to the first two might derive from the difficulty of attributing a cyber operation – cyber-attack – to a state

[23] Max Smeets, and Herbert S. Lin, "Offensive Cyber Capabilities: To what ends?," *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE (2018): pp 55-72, http://dx.doi.org/10.23919/CYCON.2018.8405010, 61.

[24] Nadiya Kostyuk, and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* 63.2 (February 2019): pp 317-347, https://doi.org/10.1177/0022002717737138, 321.

[25] Richard B. Gasparre, "The Israeli 'E-tack' on Syria – Part II," AIRFORCE TECHNOLOGY, March 10, 2008. https://www.airforce-technology.com/analysis/feature1669/.

[26] Schulze, "Cyber in war," 191.

actor. In a war context, the issue of attribution remains central as it may trigger further measures – such as retaliation – by the counterparts. When it comes to cyberspace, attribution must be assessed both on a *technical* level and on the *legal* one. Lin defines technical attribution as “the ability to identify the party responsible for an offensive cyber operation based only on technical indicators and information associated with that operation”.[27] Here, the focus narrows down to the identification of two elements: a) the *technological tools* used in the attack, meaning that the malicious cyber activity is attributed to a specific machine, computer, IP address etc.; b) the *human intruder* who carried out the attack, meaning their identity. On the other hand, Lin develops further tackling the question of “*who is to blame?*” instead of the previous “*who did it and through which instrument?*”, thus introducing the attribution of a cyber activity to an *ultimate responsible party* – i.e. an organisation, a movement, a national government etc.[28] In case the answer to the question is “a state actor” or “a state”, the consequences on a legal and political level for the attacker, the attacked and the international community become even more significant. To assess such responsibility, technical indicators are not sufficient anymore: other elements coming from international conventions and international law play a much bigger role in determining whether an individual was acting on behalf of their government or *ultra vires*, if the said government was acting beyond its lawful rights and should be held responsible for an illegal use of force, or if there was any circumstance precluding wrongfulness, etc. In other words, the law of state responsibility and the attribution of internationally wrongful acts come into play.

Attribution remains, at the international level, a timeless issue for any kind of breach. The difficulties that arise in attributing a specific action to a state actor – and thus to the state itself – are only exacerbated by cyberspace’s ever-evolving and elusive nature. As seen, this leads to a greater attribution gap between *kinetic* offensive operations – abundantly retraced in all the three levels of war, and *cyber* ones – scarce and limited to the strategic and operational levels. This lack might be

[27] Lin, “Offensive Cyber Operations and the Use of Force,” 77.

[28] Herbert Lin, “Attribution of Malicious Cyber Incidents,” *Hoover Working Group on National Security, Technology, and Law,* Aegis Series Paper No. 1607 (September 26, 2016): pp 1-56, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf, 11-13.

filled in the future due to the increasing usage of cyber attacks, which will provide more elements and specifics needed to deepen and eventually complete the puzzle. The collection of data regarding cyber activities has in fact progressively become a standard practice for cyber-security firms and intelligence agencies. In the future, information-gathering might play a fundamental role in the prevention, recognition or attribution of incoming cyber attacks, net of hackers' developing abilities.

Conclusions

This paper explores the structures that enabled cyberspace to become a fertile ground for offensive military operations. The first section frames these two concepts to develop a thorough and sensitive analysis. Kuehl's definition of cyberspace takes into account the fundamental elements of this domain, enabling it to connect with the military sphere. In this sense, the use of cyberspace for both offensive and defensive goals marks the official militarization of the domain.[29] Furthermore, the attention has been specifically referred to the Offensive Cyber Capacities, outlining the essential traits of this concept.

Taking the cue from that theoretical framework, the second section contrasts the kinetic and the cyber domains of military offences. The concept of violence emerges first as worthy of review. The analysis highlights that a vast share of International Relations literature relies on a quite narrow understanding of "violence", reducing it to mere lethal bodily harm. In this way, many OCCs are thus labelled as non-violent, while, on the contrary, their non-physical impact can be quite disruptive if not destructive. This restrictive narrative is thus detrimental, it increases the distance between traditional war means and cyber-attacks nonetheless compromising the understanding of the latter and the possibility to build effective counter-structures.

At the empirical level, it is instead possible to observe differences between *kinetic* military operations, deployed under the three levels since ancient times, and *cyber* capabilities, retraced only

[29] Miguel Alberto N. Gomez, "Arming Cyberspace: The Militarization of a Virtual Domain," *Global Security & Intelligence Studies* 1.2 (Spring 2016): pp 42-65, https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain_54871.pdf, 43.

in the strategic and operational level. The challenge in classifying an OCO is also linked to the difficulty of attributing the responsibility of a cyber-attack to a State, as it exacerbates the timeless issues of attribution under international law by applying it to cyberspace's ever-evolving and elusive nature. In the future, the widespread of cyber operations carried out by different actors might continue to feed cyber-security firms and intelligence agencies' databases, thus enabling the attribution of a growing number of cases as states' cyber military operations.

Bibliography

Arquilla, John. “The Rise of Strategic Cyberwar?” ACM, September 25, 2017. https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext.

Baezner, Marie, and Patrice Robin. “Stuxnet” (No. 4). Center for Security Studies (CSS), ETH Zürich (October 2017). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs Cyber-Reports-2017-04.pdf.

Brantly, Aaron, and Max Smeets. “Military Operations in Cyberspace.” In *Handbook of Military Sciences*, eds Anders McD Sookermany, 1-16. Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-02866-4_19-1.

Butts, Jonathan, and Michael Glover. *Developing a Tactical Environment Cyber Operations Training Program*. MCKELLAR CORP VIRGINIA BEACH VA (January 2015). https://apps.dtic.mil/sti/pdfs/ADA624747.pdf.

Calderaro, Andrea, and Anthony J. Craig. “Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building.” *Third World Quarterly* 41, no. 6 (March 19, 2020): 917–38. https://doi.org/10.1080/01436597.2020.1729729.

Carr, Jeffrey. *Inside cyber warfare: Mapping the Cyber Underworld*. O'Reilly Media, Inc., 2012.

Deibert, Ronald J., and Rafal Rohozinski. “Risking Security: Policies and Paradoxes of Cyberspace Security.” *International Political Sociology* 4, no. 1 (March 2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Egloff, Florian J., and James Shires. “The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence.” *European Journal of International Security* (October 12, 2021): 1–20. https://doi.org/10.1017/eis.2021.20.

Fanelli, Robert. “Cyberspace Offense and Defense.” *Journal of Information Warfare* 15, no. 2 (2016): 53-65. https://www.jstor.org/stable/26487531.

Gasparre, Richard B. “The Israeli ‘E-tack’ on Syria – Part II”. AIRFORCE TECHNOLOGY, March 10, 2008. https://www.airforce-technology.com/analysis/feature1669/.

Gomez, Miguel Alberto N. “Arming Cyberspace: The Militarization of a Virtual Domain.” *Global Security & Intelligence Studies* 1.2 (Spring 2016): 42-65. https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain_54871.pdf.

Harknett, Richard J., and Max Smeets. “Cyber Campaigns and Strategic Outcomes.” *Journal of Strategic studies* 45, no. 4 (March 4, 2020): 534-67. https://doi.org/10.1080/01402390.2020.1732354.

Kostyuk, Nadiya, and Yuri M. Zhukov. “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?.” *Journal of Conflict Resolution* 63.2 (February 2019): 317-47. https://doi.org/10.1177/0022002717737138.

Kuehl , Daniel T. (2009). “From Cyberspace to Cyberpower: Defining the Problem,” In “Cyberpower and National Security”, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. National Defense University Press, 2009.

https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

Lin, Herbert. “Attribution of Malicious Cyber Incidents,” *Hoover Working Group on National Security, Technology, and Law*, Aegis Series Paper No. 1607 (September 26, 2016): 1-56. https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4 (2010): 63-86. https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

Maurer, Tim. “The Case for Cyberwarfare” Foreign Policy, October 20, 2011. https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of strategic studies* 35.1 (2012): 5-32. https://doi.org/10.1080/01402390.2011.608939.

Sanger, David & Mark Mazzetti. “U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict.” *New York Times,* February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Schulze, Matthias. “Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations.” *2020 12th International Conference on Cyber Conflict (CyCon)*, Vol. 1300, IEEE (2020): 183-97. https://doi.org/10.23919/CyCon49761.2020.9131733.

Smeets, Max, and Herbert S. Lin. “Offensive Cyber Capabilities: To what Ends?.” *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE (2018): 55-72. http://dx.doi.org/10.23919/CYCON.2018.8405010.

Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge University Press, 2016.

Stone, John. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36, no. 1 (November 29, 2012): 101-8. https://doi.org/10.1080/01402390.2012.730485.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, Washington, D.C., U.S.A., 2011: 1-13. https://www.defense.gov/news/d20110714cyber.pdf.

Zdzikot, Tomasz. “Cyberspace and Cybersecurity.” *Cybersecurity in Poland*. Springer, Cham (2022): 9-21. https://doi.org/10.1007/978-3-030-78551-2_2.