DIGITAL BLOCKADE OR CORPORATE BOYCOTT?

A NEW TACTIC OF WAR

Alison Lawlor Russell

The Ukraine-Russia war is both an information war and a conventional military war. The effects of the bombs, tanks, and missiles are brutal and undeniable as are the effects of competing social media and digital public relations campaigns. Existing literature on blockades in the cyber domain is closely tied to the empirical evidence of a few cases. The events in Ukraine provide additional evidence and improve the understanding of blockade operations in cyberspace, corporate boycotts, and what could be termed digital exclusion zones.

When Russia invaded Ukraine on February 24, 2022, Ukraine's Vice Prime Minister and Minister of Digital Transformation Mykhailo Fedorov launched a technology campaign against Russia. Before the war, he led an effort to digitize Ukrainian social services. Fedorov, a former technology entrepreneur and campaign director for digital outreach for candidate Volodymyr Zelenskyy, implemented this multipronged effort to protect and defend Ukraine and retaliate against Russia in cyberspace. Using Twitter and other social media, Federov urged multinational technology companies (MNCs) such as Apple, Google, Netflix, Intel, PayPal, and others to cease conducting business in Russia, aiming to sever it from the world economy and the global internet.

Fedorov helped organize a team of volunteer hackers to create chaos on Russian websites and online services and then built an "IT Army" to neutralize and counterpunch Russian cyberattacks on Ukraine. His office also created a cryptocurrency fund to raise money for the Ukrainian military. For these efforts, Fedorov was credited with creating a new playbook for technology in war, particularly in a war against a formidable aggressor.[1]

The Ukraine-Russia war is both an information and conventional military war. The effects of the bombs, tanks, and missiles are brutal and undeniable. But the social media campaigns and digital public relations campaigns have kept the conflict at the center of the world's focus, sharing images and videos of what is happening on the

Dr. Alison Lawlor Russell, chair of the Political Science and Public Policy department and director of the International Studies Program at Merrimack College, North Andover, Massachusetts, is the author most recently of Strategic A2/AD in Cyberspace *(2017).*

1. Adam Satariano, "Shaming Apple and Texting Musk, a Ukraine Minister Uses Novel War Tactics," *New York Times*, March 12, 2022, https://www.nytimes.com/.

ground, and mobilizing public support for Ukraine and against Russia.[2] Ukraine cannot win the conventional military war without international public support, including political, economic, and military aid. Similarly, it is unlikely to be victorious without a savvy information campaign designed to keep the world's focus on Russia's aggression and Ukraine's suffering and heroism. In galvanizing the world community, the campaigns have portrayed Russia's aggression as an attack on the international system, not just the territorial sovereignty of Ukraine.

Fedorov has created a digital blockade to make life so inconvenient for Russian citizens that they will not support the war.[3] But what does a digital blockade mean? Are the actions of the technology companies involved significant, and if so, why? How can this be understood in the context of cybersecurity theory? Misnaming or conflating actions with something they are not may lead to a lack of clarity about a problem, inadequate resources, and an inappropriate response. The existing literature on blockades in the cyber domain is closely tied to the empirical evidence of a few cases. The events in Ukraine provide additional supporting evidence; examining these events may improve the understanding of blockade operations in cyberspace.

Multinational technology corporations are engaging in a novel way in international conflict by leveraging their influence over society and government. This phenomenon needs to be analyzed for its similarities to other actions such as blockades, and its implications must be considered more broadly for the role of MNCs in international conflict. This article will analyze events in Ukraine's digital blockade to update and refine the digital blockade theory, making it more applicable and relevant to innovations in international relations. This analysis will also help clarify the digital events related to Ukraine. If these events do not meet the criteria of a blockade, a more accurate term should be used to describe them and explore their implications.

Background

Russia's cyberattacks on Ukraine started on January 14, 2022, with the first attacks affecting about 70 Ukrainian government websites. Many sites were defaced and included the message to Ukrainian citizens to "be afraid and expect the worst."[4] While the websites were restored within a few hours, the attack hinted at what would come. About a month later, another cyberattack targeted Ukraine's defense ministry and two state-owned banks, Privatbank and Oschadbank. This distributed denial-of-service attack lasted less than 24 hours but impacted service during that time.[5] These attacks proved to be the prelude to Russia's military invasion of Ukraine.

2. Satariano, "Shaming Apple."

3. Satariano, "Shaming Apple."

4. "Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv," BBC News, January 14, 2022, https://www.bbc.com/.

5. "Ukraine Banking and Defense Platforms Knocked Out amid Heightened Tensions with Russia," Netblocks, February 15, 2022, https://netblocks.org/; and The Cube, "Ukraine's Defence Ministry and Two Banks Targeted in Cyberattack," Euronews, February 16, 2022, https://www.euronews.com/.

On February 24, 2022, Russian forces invaded Ukraine. Two days after the war began, Fedorov asked Meta to ban access to Facebook and Instagram in Russia. Meta declined, citing the need for protestors to use the site to organize against the war and provide independent information, but it did agree to label and fact-check posts by Russian-controlled state media. Fedorov also asked YouTube to block Russian propaganda media, and YouTube responded by blocking more than 900 Russian channels and taking down more than 70,000 videos for violating its content guidelines, such as referring to the invasion as a "liberating mission."[6] Federov continued asking technology companies to withdraw from Russia to create a "digital blockade."[7] As of early April 2022, more than 600 companies had withdrawn their services from Russia.[8]

While foreign technology companies were withdrawing services to Russia, the Russian government was blocking access to those sites. Meta restricted access within the European Union to state-controlled media outlets Russia Today and Sputnik and labeled postings from the Kremlin or other official government outlets. In retaliation, Russia banned Facebook and Instagram from the country.[9]

The Russian government also blocked independent media outlets in Russia—such as Echo of Moscow, an influential radio station; Dozhd; TV Rain, Russia's only independent television station; and Meduza, an English- and Russian-language news website—because of their war reporting. The government also blocked foreign sites such as the BBC Russian Service and other international Russian-language programs because of their coverage of the war in Ukraine. These restrictions caused the loss of independent programming for millions of people inside and outside Russia.[10]

The United States began imposing sanctions on Russia on February 22, 2022.[11] Within six months, more than 1,000 companies had voluntarily curtailed operations in Russia beyond the minimum legal requirements of international sanctions. Some companies continue to operate in Russia undeterred, but an unprecedented number of companies chose to leave or suspend operations when they were not compelled to by law.[12] These firms collectively represent about 40 percent of Russia's gross domestic

6. Laurens Cerulus, "Ukraine's Digital Minister Pleads with Big Tech to Pressure Moscow," *Politico*, February 26, 2022, https://www.politico.eu/article/; and Dan Milmo, "YouTube Removes More Than 9,000 Channels Relating to Ukraine War," *Guardian*, May 22, 2022, https://www.theguardian.com/.

7. Satariano, "Shaming Apple."

8. Jeffery Sonnenfeld et al., "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain," Chief Executive Leadership Institute, Yale School of Management, updated February 5, 2023, https://som.yale.edu/.

9. Ryan Mac, Mike Isaac, and Sheera Frenkel, "How War in Ukraine Roiled Facebook and Instagram," *New York Times*, March 31, 2022, https://www.nytimes.com/.

10. "Russia: With Tech Firms Pulling Out, Internet Spiraling into Isolation," Human Rights Watch (website), March 14, 2022, https://www.hrw.org/; and "BBC, CNN, and Other Global News Outlets Suspend Reporting in Russia," *Guardian*, March 4, 2022, https://www.theguardian.com/.

11. "Sanctions Framework," Russia-Country Commercial Guide, International Trade Administration, US Department of Commerce (website), updated July 21, 2022, https://www.trade.gov/.

12. Sonnenfeld et al., "Over 1,000 Companies."

product.[13] The list of technology companies that have now withdrawn from Russia include major corporations such as Qualcomm, Intel, Sony, Google, IBM, Microsoft, Cisco, PayPal, Apple, Meta, Oracle, Twitter, TikTok, and SnapChat.[14]

Four days after the Russian assault on Ukraine began, the Ukrainian government asked the Internet Corporation for Assigned Names and Numbers (ICANN) to cut Russia off from the global internet. Specifically, it asked for the country code .ru and its Cyrillic equivalents to be revoked. The corporation rejected the request as "neither technically feasible nor within its mission."[15] Gören Marby, ICANN chief executive officer, went on to explain, "ICANN has been built to ensure that the Internet works, not for its coordination role to be used to stop it from working."[16]

Ukraine has also advocated for Russia's removal from the International Telecommunication Union (ITU). Ukraine views Russian access to the ITU as "an international security priority."[17] The Ukrainian government has called for cutting off Russia's access to any hardware or software that could allow Russia to upload and disseminate malware and viruses. Ukraine lobbied the United States and other allies to include telecommunications products such as software and microelectronics in sanctions so that Russian systems could not be updated or repaired during the conflict.[18]

Russia's removal from the International Telecommunication Union would send a clear message and cut off Russia's access to technical information and innovation. The ITU's international standardization process encourages innovation in both large and small businesses, market leaders, and followers. To participate in the standardization

13. Jeffrey Sonnenfeld and Steven Tian, "Zelensky Unplugged: Ukraine's President Gives American CEOs Advice and Sobering Warnings about 'Our Common War,' " *Fortune*, June 14, 2022, https://fortune.com/.

14. Natalie Huet and Pascale Davies, "Which Tech Companies Are Cutting Ties with Russia over Its War in Ukraine?," Euronews, March 17, 2022, https://www.euronews.com/.

15. Brian Fung, "Ukraine's Request to Cut Off Russia from the Global Internet Has Been Rejected," CNN, March 3, 2022, https://www.cnn.com/.

16. Fung, "Ukraine's Request."

17. Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/.

18. Raphael Satter, "Ukraine Lobbies US Officials for Bans on Russia Software, Aviation-Diplomat," Reuters, February 24, 2022, https://www.reuters.com/; Bureau of Industry and Security (BIS) Office of Congressional and Public Affairs, "Six Months into Russian Invasion, Commerce Actions Making a Difference in Support of Ukrainian People," press release, US Department of Commerce BIS (website), August 25, 2022, https://www.bis.doc.gov/; and Iryna Bogdanova, "The Role of Technology Sanctions in Crippling Russia's War Machine," International Institute for Sustainable Development (website), September 26, 2022, https://www.iisd.org/.

process, members must have the technical expertise to know how things are made or done, and it is an opportunity for businesses and subject matter experts to learn from each other and potentially shape new standards in their favor.[19]

Ukraine seeks to restrict Russian access to software that will be installed on servers as a way of restricting its access to those services globally. The innovation sharing and research that come with membership and attendance at conferences are valuable and sometimes critical to maintaining technical standards and compliance; if Russia were removed from the ITU, it would lose access to this information. Without modern information technology developments, Russia could not install its software on modern hardware. It is a slow process, but Ukraine wants Russia to stagnate technically while Ukraine continues to advance.[20]

Theoretical Foundations for Digital Blockades

Blockades have a specific definition in international law, and Federov has called the actions of technology companies regarding Russia a "digital blockade." But is it a blockade, and if not, what is it? International law roots its understanding of blockades in naval operations. Naval blockades are the offensive regulation of trade during wartime. Their purpose is "to isolate the enemy in such a fashion as to destroy its import and export trade."[21]

Blockades can also occur on land, in air, in cyberspace, and possibly in space. A cyberspace blockade is defined as "an attack on cyber infrastructure or systems that prevents a state from accessing cyberspace, thus preventing the transmission (ingress and egress) of data beyond a geographical boundary."[22] As coercive operations of war, blockades are designed to achieve military advantages and diplomatic advantages. Diplomatic advantages include creating financial constraints, isolating the adversary politically, rendering society uncomfortable and inconvenienced in order to influence policy, or demonstrating relative power and capabilities to influence negotiations.

Blockades in cyberspace share a critical feature with actions that are recognized as blockades in other domains, namely, preventing the ingress and egress of normal traffic—ships, aircraft, land vehicles, or data packets—in that domain beyond a specific geographic area. The actors involved are usually but not exclusively states. Blockades require certain technological capabilities, knowledge of the domain, and knowledge of the opponent's vulnerabilities and capabilities.

Furthermore, blockades almost always occur during war or extant conflict. In blockade operations, neutral parties should not be targeted and have rights that

19. Johan Bjerkem and Malcolm Harbour, "Europe as a Global Standard-Setter: The Strategic Importance of European Standardisation," discussion paper, Europe's Political Economy Program (Brussels: European Policy Centre, October 15, 2020), 6-7, https://www.epc.eu/.

20. Rosen, "Man at the Center."

21. Maurice Parmelee, *Blockade and Sea Power: The Blockade, 1914–1919, and Its Significance for a World State* (New York: Thomas Y. Crowell Company, 1924), 7.

22. Alison Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 5.

should be protected, although unintended consequences can occur.[23] Naval blockades, aerial blockades, and land blockades are all considered acts of war according to international law. Moreover, there is support in the international community to consider blockades in cyberspace acts of war as well.[24]

International law maintains an important distinction between blockades and exclusion zones, which is relevant for the digital blockade campaign against Russia. Blockades prevent data from traversing a boundary, whereas exclusion zones focus on the activities that take place within a specific geographic area. Exclusion zones, or areas of denial, are areas in which a state that is actively engaged in war, also known as a belligerent, possesses "the ability to degrade, deny, or destroy the adversary's freedom of action within the contested area."[25]

Blockades deny access to an area while exclusion zones deny operations within that area. They are often used in tandem as they can be mutually reinforcing and effective at achieving the goal, which is dominance of the domain, but they are separate operations. Thus, an aerial blockade prevents aircraft from crossing a border, while an aerial exclusion zone—a no-fly zone—prevents the movement of aircraft within that border. If Ukraine could block aircraft from leaving Russia, it would not need a no-fly zone over Ukraine. Despite the technical and legal distinction between these two concepts, scholars, practitioners, and policymakers alike frequently use them interchangeably. For a time, the US military itself combined these two concepts into the term "anti-access/area-denial" or "A2/AD" operations.

A cyber (or digital) exclusion zone could also be implemented. Prior work has examined how a cyber exclusion zone could be conducted at the physical (e.g., hardware) layer or the logic (e.g., networks) layer of cyberspace (fig. 1). The choice of cyber instead of digital is deliberate in this instance. Cyberspace encompasses satellites and other technology that is broader than the internet. Digital typically refers to internet-based activities and therefore may not be broad enough to encompass the full spectrum of cyber capabilities. Earlier scholarship details how submarine and terrestrial cables, satellites, and the electromagnetic spectrum could all be leveraged to create either a blockade or an exclusion zone at the physical layer. At the logic layer, root servers, border gateway controls, and internet service providers could be manipulated to deny service or access to a region.[26]

These types of exclusion zones, imposed at the physical or logic layer, could prevent someone inside the region from conducting activities in cyberspace, either digitally online or via satellites. The exclusion zones at the physical or logic layers could be created through digital attacks, such as blunt distributed denial-of-service attacks, more

23. Russell, *Cyber Blockades*, 63.

24. Michael N. Schmitt, ed., *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), 195–98.

25. Alison Russell, *Strategic A2/AD in Cyberspace* (Cambridge: Cambridge University Press, 2017), 3.

26. Russell, *Strategic A2/AD*, 26–52.

sophisticated command-and-control attacks, or in extreme cases, through the physical manipulation or destruction of the necessary hardware.

Depending on the way an exclusion zone is implemented, it may or may not be easy to cease or reverse the operation, and it may have significant effects on the post-conflict environment. If physical infrastructure is destroyed, economic, political, and social recovery takes time, whereas these activities might resume immediately following the conclusion of a targeted offensive cyber operation.

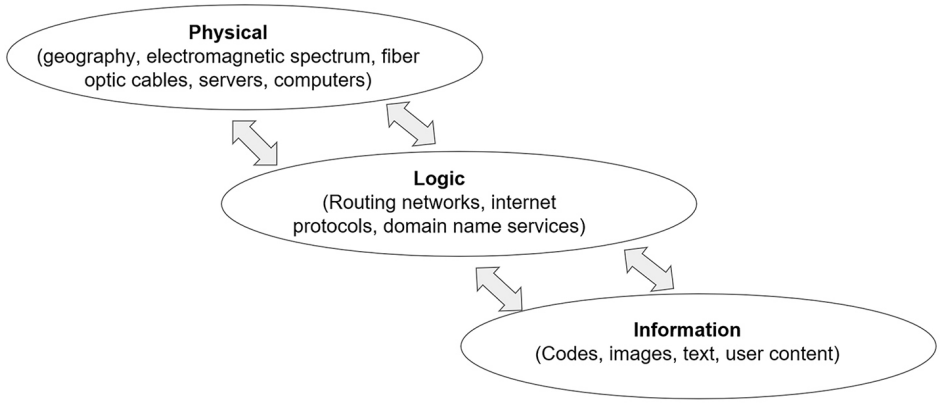

Figure 1. Layers of cyberspace

The extant literature on digital or cyber blockades does not address blockades or exclusion zones that take place at the information layer of cyberspace (fig. 1). The majority of internet users are only vaguely aware of the physical or logic layers of cyberspace. For most users, the information layer of the internet is what they see on their screens: applications and websites that help them interface with emails, texts, photos, navigational systems, social media, banks, government services, and many other facets of modern life. [27] Cyberattacks at this level can range from unsophisticated and minor defacement attacks to sophisticated and potentially extremely damaging network intrusions. They can be very difficult to deter and prevent, and they can be conducted by a wide range of actors, from lone individuals to large government entities.

This gap in the literature addressing the information layer may be a result of the few cases of cyber blockades that have occurred thus far. Cases of blockades in cyberspace are limited to Estonia in 2007 and Georgia in 2008. But the events in Ukraine in 2022 appear to present an additional case that may provide further insights into the concept of digital and cyber blockades. Specifically, the Ukraine case offers two avenues of inquiry and examination. First, it suggests blockade-like operations can occur at the information level, which has not yet been systematically examined. Second,

27. Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma" (Explorations in Cyber International Relations Working Paper 2012–3, Massachusetts Institute of Technology Political Science Department, Boston, MA, 2012), https://hdl.handle.net/.

it suggests the level of analysis must go beyond state actors and state-sponsored actors to include the role of multinational corporations.

Digital Blockade of Russia

In the so-called digital blockade of Russia, the Ukraine government called on global technology companies to sever ties and services to Russia. Clearly, as private companies, corporations can choose where they do business notwithstanding government embargoes or other legal restrictions. At Ukraine's request, some multinational corporations reduced or suspended their business operations in Russia. The request and subsequent responses were conducted in the context of an armed conflict in which Russia violated international law and invaded Ukraine. Ukraine and Russia are the sole belligerents, but the technology companies called upon to boycott Russia are in other countries, many of which have provided political, economic, and military support for Ukraine.

Blockades in different domains are historically defined by certain common elements that provide the legal basis for recognizing a blockade.[28] Under the first criterion, a defining action must occur: blockades involve preventing all vessels and traffic—enemy and neutral—from entering specified ports or areas that are controlled by the enemy belligerent state.[29] The actions taken against Russia by multinational technology companies prevent the entry or exit of data. But although they cease the flow of their data and services, they do not prevent anyone else from transmitting data. If the Internet Corporation for Assigned Names and Numbers had cut off access for all domains that ended in .ru, it would have forcibly prevented access to any actor; however, it has not done so. Accordingly, the first criterion is not met.

The second criterion concerns the actors involved. According to international law, belligerent states, specifically armed forces, participate in blockades.[30] Because a blockade is an act of war under international law, only states can conduct one.[31] In a few cases, actors that are not or were not internationally recognized states have been parties to blockades, but these instances have been rare and have usually involved self-governing territories that wished to be recognized internationally as states, such as contemporary Palestine and the nineteenth-century Confederate States of America. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* clarifies that "non-state actors are not entitled to establish a naval, aerial, or, a fortiori, cyber blockade."[32] Because multinational corporations are the ones attempting to conduct the blockade action in this case, this criterion is not met.

28. Schmitt, *Tallinn Manual*, 196; and Russell, *Cyber Blockades*, 62–64.
29. Schmitt, 195; and Russell.
30. Schmitt, 196; and Russell.
31. Schmitt, 198; and Russell.
32. Schmitt.

The third criterion is the capability to enforce an effective blockade. Blockades must be enforceable and reasonably effective in their domain.[33] In the case of the actions against Russia, the actions were not designed to prevent the flow of all or even a majority of data. Consequently, these actions have not been effective as blockades, and thus, this criterion is not met.

The fourth criterion is the presence of conflict. As an interaction between belligerents often involves armed forces, the presence of conflict or a declaration of war usually either precedes or immediately follows a blockade. International law also specifies that the blockades must be declared, which is almost the same as declaring war, since blockades are acts of war.[34] Armed conflict exists at the level of interstate war between Russia and Ukraine, and it was this war that led to the actions against Russia, so this criterion is met.

In the fifth and final criterion, the blockade must be impartial and respect the rights of neutral parties—states.[35] In this case, the rights of neutral states were not violated because data from neutral states were not blocked. Also, the technology companies acted as private companies and not on behalf of their home countries, and they did not provide direct material support to either belligerent. Their actions may have aided Ukraine, but they did not violate the neutrality of their home countries or other states. This criterion is therefore met.

Under this analysis, the digital blockade of Russia does not satisfy the criteria for a blockade under international law because it does not forcibly prevent the ingress and egress of traffic, it is not conducted by belligerents, and it is not effective and enforceable. As such, the actions against Russia are a different type of action and cannot be sufficiently addressed by adjusting the definition or theories of blockades. Furthermore, the actions against Russia represent a difference in kind, not degree. Still, if it is not a blockade, what should it be called? The terminology should address what the actions accomplish and the implications for the international system.

Corporate Boycotts

One possibility is to identify the actions undertaken by multinational technology corporations as a corporate boycott. Boycotts are usually led by consumers who refuse to conduct business with an individual, group, or company to protest the target's behavior, inflict economic losses, indicate moral outrage, and/or induce the target to change its behavior. Boycotts can also be led by companies that refuse to do dealings with customers, such as governments or countries, for the same reasons and goals. Technology companies are particularly well-suited to conduct boycotts because they can reach a large audience, and their products tend to be well integrated into the social, political, and economic lives of the consumers.

33. Schmitt, 196; and Russell.
34. Schmitt; and Russell.
35. Schmitt; and Russell.

The collective activities undertaken by multinational corporations against Russia at the request of the Ukraine government represent a corporate boycott, defined here as a situation where corporations refuse to conduct business operations in a country in response to that country's policies or actions. In this case, corporations are refusing to conduct business in Russia because of the Russia's invasion of Ukraine.

This is a new phenomenon, and the terminology is not settled. Some scholars refer to it as a "business retreat" or a "business withdrawal," but due to the large scale and political motivation of the actions, this article favors corporate boycott as the best term to describe the phenomenon.[36] This corporate boycott complements national boycotts and sanctions and terminates the sale of their goods or services in Russia. It is voluntary for companies to participate in the boycott, and the boycott is widespread, with many industries and hundreds of companies participating.

Still, some companies have chosen to remain on the sidelines for specific reasons. For example, Cloudflare continues to operate in Russia because, according to Chief Executive Officer Matthew Prince, shutting down in Russia would have adverse effects on society, particularly dissidents, and ultimately be beneficial to the Russian government.[37] Other companies argue boycotts create an opportunity for the Russian government to exert more control over Russian people, which is counterproductive, or that boycotts are ineffectual because they will economically hurt only innocent people instead of the government or military.[38]

A corporate boycott on the scale of the one in Russia and under these circumstances is a rare and perhaps unprecedented event. In the 1980s, government boycotts, corporate boycotts, and divestment campaigns were waged against South Africa in protest of apartheid. But there has not been an event like the Russian invasion of Ukraine in recent decades, nor has there been a corresponding corporate boycott. Additionally, boycotts decades ago predated the information and communications technology systems that underpin contemporary financial, business, social, government, and military functions. Therefore, this boycott is the first of its kind—a voluntary corporate boycott of digital services directed against a strong country in retaliation for its aggression and violation of international law.

The corporate boycott is designed to draw attention to Russian government aggression, satisfy the moral outrage of global consumers and stakeholders, and impose costs on the lives of the Russian people so they pressure their government to change its policy. It is not a short-term solution but a long-term pressure campaign. Akin to norm development, the corporate boycott seeks to counter Russian President Vladi-

36. Sonnenfeld et al., "1,000 Companies"; and Jeffrey Sonnenfeld et al., "Business Retreats and Sanctions Are Crippling the Russian Economy," Social Science Research Network (SSRN), July 19, 2022, http://dx.doi.org/.

37. Aimee Chanthadavong, "Cloudflare and Akamai Refuse to Pull Services out of Russia," ZDNet, March 8, 2022, https://www.zdnet.com/.

38. William MacAskill, "Does Divestment Work?," *New Yorker*, October 20, 2015, https://www.newyorker.com/.

mir Putin's propaganda and increase pressure to return to the post-1945 international rules of nonaggression.

Importantly, the war in Ukraine is being interpreted as more than simply a war between countries. Nations and international organizations are perceiving it as Russia's challenge to the international system.[39] The international system includes multinational corporations that operate within the current system, following its laws and norms. Thus, while not belligerents and not parties to the conflict, MNCs can impose costs—sanctions—on countries that threaten international law and global stability. This appears to be what these businesses are attempting to do with this corporate boycott.

Ultimately, this boycott is a new phenomenon in the panoply of international relations: MNCs, acting en masse and independent of state or government instruction, can deny access to information, goods, and finances for an entire country without endangering the neutrality of their home country.

This research, then, raises new questions about the role of multinational corporations in war. Large corporations, particularly technology companies, are integral to the global economy, the domestic function of states, and the ability of military forces to operate effectively. The role of MNCs matters because those companies may seek protection from the government from hackers or belligerent states, and they may need to respond if they are targeted by adversaries in retaliation for their corporate actions. Lastly, attacks on major actors in the international cyberspace ecosystem, such as technology companies, may require a coordinated, comprehensive response that involves multiple corporations as well as the government.[40]

Implications of Corporate Boycotts for Conflict

Blockades in cyberspace have previously been conducted at the logic layer because it is easier for state actors to control access to information at that level, which is upstream from the information layer (fig 1).[41] The logic layer tells computers which routes to follow to create a pathway for a request for information to be fulfilled. The information layer is downstream in that it relies on the physical and logic layers to provide the structure for sharing information in cyberspace. The information layer is much more diffuse and disparate, and is the focus of defacement, phishing, or ransomware campaigns. If a state wanted to conduct a blockade in cyberspace, the infor-

39. Robert Pszczel, "The Consequences of Russia's Invasion of Ukraine for International Security—NATO and Beyond," *NATO Review*, July 7, 2022, https://www.nato.int/; Stefan Meister, "A Paradigm Shift: EU-Russia Relations after the War in Ukraine," Europe's East Project, Carnegie Europe (website), November 29, 2022, https://carnegieeurope.eu/; UN General Assembly Resolution, Aggression against Ukraine, A/ES-11/L.1 (March 1, 2022), https://www.documentcloud.org/; and Lise Morjé Howard, "A Look at the Laws of War — and How Russia Is Violating Them," Analysis and Commentary, United States Institute of Peace (website), September 29, 2022, https://www.usip.org/.

40. Brad Smith, "Foreword," in *Defending Ukraine: Early Lessons from the Cyber War*, Microsoft, June 22, 2022, 1–4, https://blogs.microsoft.com/.

41. Russell, *Cyber Blockades*, 69–127.

mation layer presents challenges because the outlets are so numerous that it would be resource-intensive to deny access to information as it is provided.[42] As a result, a true blockade in cyberspace led by one state against another state is unlikely to occur at the information level.

A corporate boycott in the technology sector is another way to achieve effects similar to a cyber blockade but at the information layer and without state involvement. Corporate boycotts, when conducted en masse against a country, can deny the country access to information and services in cyberspace. As a corporate boycott, the action is the result of the decision of private companies, and it cannot constitute an act of war. Yet it achieves the result of disrupting and perhaps even preventing access to information and services in cyberspace. Multinational corporations have the freedom to decide where to conduct business, and they are free to sever or downgrade business relationships for any reason, including profits, stability, or politics.

Private companies acting together can create what is effectively a digital exclusion zone. Unlike other types of digital exclusion zones such as domestic censorship or internet "kill switches" that are frequently discussed in connection with authoritarian regimes, providers of content and services can create digital exclusion zones by refusing to provide services to a country. Usually, technology companies seek to expand their services and market reach; it is notable, therefore, that in the case of Russia, dozens of MNCs have chosen to reduce their services and market reach because of a conflict to which they are not directly parties.

According to international law, only states can be considered belligerents in warfare. Thus, by definition, MNCs cannot impose a blockade. Moreover, while MNCs engaging in a type of digital exclusion zone may have the ability to unilaterally cut off the flow of data or digital services that impact the political, financial, and social life of a country's population, for the reasons stated previously, this does not constitute a blockade. If a state ordered companies to undertake these actions, and the state were belligerent to the conflict, the result may constitute a blockade.

Yet, while multinational corporations cannot impose a blockade, they can withhold action through a boycott. If an MNC holds a monopoly position in a vital sector, a boycott might result in a strangulation. A strangulation is the extreme edge of the same discomfort-to-force-policy-change that is the purpose of boycotting. The extreme edge may be unlikely, but it is based on the same principles. Moreover, in the case of Ukraine, Russia is the clear aggressor in the war. Yet it may not always be obvious who the aggressor is, and the ability of an MNC to potentially conduct strangulation of a country without the involvement or support of a state is new and has further implications of its own.

A corporate boycott, digital or otherwise, represents innovative statecraft that involves different actors—MNCs—than blockades to help states achieve their goals. The resulting economic pressure occurs below the threshold of warfare in the gray zone but can have important consequences for the outcome of a conflict. The actions do not nec-

42. Russell, *Strategic A2/AD*, 40–52.

essarily broaden a conflict but instead tap into sympathy and moral support that allow noncombatants to help support combatants in meaningful ways. This is a nonviolent way for nonstate actors who are members of the international community to apply pressure to a state that has blatantly violated international norms and created instability. In this way, MNCs are supporting an international system that benefits them.

Conclusion

The concept of a digital blockade raises interesting questions about the conflict in Ukraine, what this so-called blockade accomplishes, and the implications for the international system. But the actions by MNCs in Russia do not satisfy the criteria for a blockade under international law. The (mis)labeling of the MNCs' actions as such reveals the shortcomings of current terminology; much of the language of war in international law—blockades, zones, sanctions, and quarantines—concerns actions all rendered by states against states. Commercial entities have not taken actions such as these independently in modern history until now, and the terminology has not evolved to explain and define these actions.

The MNCs' actions against Russia examined in this article are more appropriately called a digital corporate boycott instead of a digital blockade. This type of action, undertaken below the threshold of armed conflict, allows powerful actors not beholden to states to act independently in an active conflict to try to influence the outcome. The idea of corporations supporting one side in a conflict is not new, but the scale of the MNCs' actions—the size of the corporations and their potential to impact the countries—is unlike anything the world has seen in modern history. The East India Companies or privateering companies would be the closest historical examples, but they differed in important ways, such as having the letters of marque or explicit approvals to conduct business on behalf of the state, including signing treaties.

Ukraine's Ministry of Technology is engaging in innovative statecraft by involving MNCs and the international community more broadly to punish Russia for its invasion. This digital corporate boycott could be very effective at making life uncomfortable for people in Russia, but it relies on the continued voluntary cooperation and action of technology companies. Because the corporate boycott targets information and society, not critical infrastructure or government operations, its specific effects will likely be difficult to pinpoint. Similar to economic sanctions, a digital boycott is not designed to apply significant pressure in the short term. Instead, its effects will manifest over a longer period of time.

More research is needed to understand the motivations and incentives for multinational corporations to become involved in geopolitical conflicts such as Russia's war in Ukraine, particularly when doing so seems to be contrary to typical market-driven behavior. The technology companies did not decide to reduce or eliminate services to Russia because they were forced into it or were provided with clear financial incen-

tives to do so. In fact, many companies lost money when they withdrew from Russia.[43] Plausible reasons for their actions include support for Ukraine, a desire to support the global consensus against Russia, and a fear of retaliation from their customers or other stakeholders if they continue to operate in Russia.

Incidentally, an ongoing debate exists over the impact of this boycott. Those tracking the withdrawal of companies from Russia assert the corporate boycott and sanctions are crippling the Russian economy. Russia has lost business with companies that are worth about 40 percent of its gross domestic product and reversed several decades of foreign investment growth. Also, a flight of capital and people has negatively impacted Russia's economic base. The sanctions, not discussed in this article, are debilitating to Russian industry. These state-supported actions have weakened Russia's position as a commodity exporter, prompted the collapse of imports, and hollowed out domestic innovation and production. As a result, Russia's financial markets performed worse than all others in the world in 2022.[44]

According to other experts, Russia is bearing up due to financial decisions to raise interest rates early in the conflict, which gave it a protective cushion.[45] Russia's relative detachment from the international economy—the West in particular—has also meant sanctions and a corporate boycott have not been as devastating as they may have been in another country. Finally, the sale of hydrocarbons has served as a financial lifeline for the Russian economy. By this accounting, the Russian economy is faring better than expected. Over time though, there is little doubt the corporate boycott and sanctions will take a toll, but it is difficult to determine exactly what the impact has been so far.[46]

Corporations have always engaged in domestic and international politics to secure their interests. The corporate digital boycott of Russia raises questions of scale and scope because multinational technology corporations have considerably more power and influence than twentieth-century corporations. For supporters of Ukraine, the involvement of technology companies to act in a coordinated fashion to pressure Russia may represent a welcome moral stand against aggression in the international community.

Before it is celebrated though, scholars must consider the implications of multinational corporations enacting a corporate boycott on the scale of a blockade. What are the risks of nonstate actors creating blockade-like effects against major states in the international system? This may lead to politically difficult and diplomatically dangerous situations for states with multinational corporations usurping or supplementing state power. Further research should be done on the motivations and rationale of the many technology corporations that acted so swiftly to sever services to Russia, so states and policymakers can better understand the circumstances under which these actions are likely to take place.

---

43. Ukrainian President Zelenskyy Addresses CEOs at Yale Summit, Yale CEO Summit, filmed by CNBC Television, streamed live on June 8, 2022, YouTube video, 1:07:46, https://www.youtube.com/.

44. Sonnenfeld et al., "Business Retreats."

45. "Bearing It," *Economist*, August 27, 2022, 59–60.

46. "Bearing It."

This corporate boycott opened a new avenue of influence or source of leverage in an armed conflict. It carves out a new role for private-sector initiatives in war and influences how the role of nonstate actors like multinational corporations should be analyzed in international security. International law does not consider this type of action because it is not conducted by a state. This perhaps points to a weakness in international law—the assumption that corporations do not or will not wield significant power independent of states. It may also affect the norms and rules for internet governance and lead to a reconsideration of the notion that private sector corporations are neutral actors.

The corporate boycott of Russia suggests technology companies believe private and public sector collaboration is necessary to counter some geopolitical threats. This shift in focus and corresponding way to fight in armed conflicts could have serious implications for governance and society as multinational corporations exercise more power in interstate conflict. **Æ**