

OCTOBER 2026

No Front Lines

A Decision Guide for Companies Caught in Conflict

AUTHORS

Emily Harding

Julia Dickson

Aosheng Pusztaszeri

A Report of the CSIS Intelligence, National Security, and Technology Program, with support from the Futures Lab

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

OCTOBER 2026

No Front Lines

A Decision Guide for Companies Caught in Conflict

AUTHORS

Emily Harding

Julia Dickson

Aosheng Pusztaszeri

A Report of the CSIS Intelligence, National Security, and Technology Program, with support from the Futures Lab

© 2026 by the Center for Strategic and International Studies.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Center for Strategic and International Studies (CSIS). CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Cover: Christopher Pike/Getty Images

Contents

Introduction: Industry on the Front Lines in Modern War	1
Decision Guide	3
<i>Step 1: Close the Information Gaps</i>	4
<i>Step 2: Discuss the Intangibles</i>	7
<i>Step 3: Assess the Risk</i>	8
<i>Step 4: Make an Initial Decision</i>	13
<i>Step 5: Develop and Stress-Test Mitigation Strategies</i>	16
The Government Stakeholders	20
Conclusion	23
Appendix 1: Gaming Out the New Reality of War	24
Appendix 2: Case Study on Microsoft in Ukraine	29
Appendix 3: Case Study on Attacks on Data Centers in the Iran War	32
Appendix 4: Complete AI Prompt	34
About the Authors	40
About CSIS	42
Endnotes	43

Acknowledgments

The authors would like to extend their gratitude to the International Committee of the Red Cross (ICRC) for their partnership on the roundtable that contributed to this research. They also wish to thank the roundtable participants and interviewees for their generous contributions. Finally, the authors would like to thank the CSIS iDeas Lab for offering their design expertise.

This report is made possible by project support from the International Committee of the Red Cross and general support.

Introduction

Industry on the Front Lines in Modern War

Industry has always played an essential supporting role in war. It builds the things that move armies, power navies, and feed and supply soldiers worldwide.¹ But today's wars are different, and the types of industries playing that supporting role have vastly expanded.

Companies that were essential to Ukraine's defense beginning in 2022 never would have considered themselves defense companies, but they rose to the challenge and helped Kyiv hold off a bigger, better-equipped foe. Tech companies in particular found themselves critical to the war effort. They are guardians of the infrastructure that civilians need to survive and that armies need to run a data-driven, real-time connectivity war—the kind of war that has proven Ukraine's strategic advantage. These companies are, in essence, on the front lines.

Iran understood this in March and April 2026. It chose to threaten not just military bases but data centers across the Gulf. AWS suffered several hits on data centers; other tech companies scrambled to find some way to defend their facilities. In our interconnected, just-in-time world, companies' missions have not changed—but war has.

Now that the lines between military and civilian use have fundamentally blurred, how should modern companies think about this new world of warfare? How should they evaluate risk when choosing whether to assist in a conflict? How do they balance the risk of becoming a target with the reputational risk of sitting on the sidelines, or choosing the wrong side?

What about governments' responsibilities? What protections can—and should—government provide? Critically, what happens when industry and government interests are aligned but there is no official relationship? And then, what happens if these interests slip out of alignment?

Now that the lines between military and civilian use have fundamentally blurred, how should modern companies think about this new world of warfare? How should they evaluate risk when choosing whether to assist in a conflict?

What follows is a decision guide for companies that find themselves lost in the fog of conflict. It walks the C-suite and the board through a set of questions that identify key knowledge gaps and then establishes a risk evaluation framework. This exercise will clear the fog. It ends with risk mitigation strategies, so that whatever the decision, the company can see around corners and minimize the chances of disaster.

In the last section, the focus switches to the government, because this is a complicated space for any administration to navigate. A decision memo for the president provides key recommendations for how the White House should evaluate risk to companies, as they are the engine of the U.S. economy and the innovation ecosystem that pushes the United States forward. It helps any administration make smart, well-crafted policies that allow companies to do good in the world while minimizing risk.

A robust set of appendices provides geopolitical context and background information on this project. They include an in-depth discussion on the war game CSIS ran to test ideas and collect data on how real-world scenarios might play out; case studies on how industry has navigated the fighting in Ukraine and Iran; and a complete version of the AI prompts suggested throughout the paper. The authors used AI to help write the AI prompts. We worked with Claude to explain what we wanted these prompts to deliver, then iterated to create the steps that would lead to precise answers. We also ran these prompts multiple times with test-case companies to further hone them.

The intended result is a way to pursue industry's mission along with the U.S. government's mission, while keeping these strategic pieces in alignment no matter what conflicts bring. Today's world has no shortage of uncertainty and turmoil. Industry and government need each other to prevail.

Decision Guide

Clearing the Fog

A clear map helps navigate even the most troubled waters. This memo is not an academic exploration of these difficult issues; instead, it is a practical, implementable guide that will help companies navigate the turbulence of a conflict. It poses tough questions with an eye toward developing honest answers to provide the best chance of positioning for success in a future fraught with risk.

In this decision guide, we have used “countries A and B” as a placeholder for the countries in conflict. Country A is a theoretical aggressor that invaded a neighbor (Country B) without provocation. The genesis for this work was Russia’s full-scale invasion of Ukraine, and the many companies that valiantly, but somewhat blindly, stepped into the breach. That said, we intentionally constructed the exercise to be applicable to a wide range of conflicts, including those where the aggressor and victim are less clear, or where the conflict is less consistently in the public eye. This map will be useful for everything from border disputes to a conflagration between major powers.

This memo is not an academic exploration of these difficult issues; instead, it is a practical, implementable guide that will help companies navigate the turbulence of a conflict.

There are five steps, summarized here and explained in detail in the following pages:

1. **Gather facts** to close the information gaps. Fully understand company exposure on the ground, high and low estimates for potential losses, and the board's tolerance for risk. Talk to outside experts (like CSIS) about the likely course of the conflict ahead.
2. Use the prompts to **have honest conversations about the intangibles**, like how company values will inform decisions. These factors will provide key context surrounding the numbers. A critical factor here is your board; you and they must be on the same page about the balance between company values and potential financial losses.
3. Use the chart on page 9 as a guide to **answer the most critical questions and firmly establish the severity of the risk**.
4. **Make a preliminary decision**.
5. Finally, **establish a mitigation strategy** for your preferred way ahead, which will stress-test that initial decision. Is the mitigation strategy unacceptably costly? Is it likely to work as intended? The difficulty of implementing the mitigation strategy should inform the final decision. **For the final stress test, engage with the board about the plan**. Brief them on the facts, intangibles, mitigation strategy, and recommended direction.

In several places, the guide suggests ways to capitalize on AI's capability to process complex data in order to help parse decisions. The guide offers draft AI prompts, which the authors tested using several commercially available systems with hypothetical company data. They are flexible—a company may want to tweak the prompts and enhance them with proprietary data on a closed system to get the most detailed answers possible.

The result of the exercise is structured thinking that shows the way through a complex, fluid, and challenging situation. For a company that finds itself suddenly drawn into a conflict, it will be an invaluable decision guide. In today's warfare, there are no clear front lines, but a company can still find a way to help itself and its customers thrive through conflict.

Step 1: Close the Information Gaps

What's the situation now?

When a crisis hits, industry leaders and policymakers alike can feel at sea, facing too many inputs but with none of the right information. Bad information leads to inefficient decisionmaking; a lack of information wastes valuable time. This section identifies the critical information leaders need in order to make accurate decisions as a crisis unfolds.

Staff should pull together a briefing book for decisionmakers that covers both halves of the picture: the best available assessment of where the conflict is headed and a detailed description of the company's posture in the affected region. The briefing book therefore poses two broad questions: What is the likely direction of the conflict? What is our posture in the combatant countries?

WHAT IS THE LIKELY DIRECTION OF THE CONFLICT?

What is our best assessment of the likely direction of the conflict? Is it likely to be a short skirmish or a long war? Is this the kind of conflict that will capture global attention for months or years, or is it likely to fade from the front pages? Will one or both sides commit war crimes and outrage the public? Put differently: How bad is bad?

War is by nature abrupt and chaotic. The fog of war is real. Early reports are almost always wrong, or at least incomplete. Many commentators become overnight experts on the latest hotspot, failing to bring deep expertise to a complex and fast-moving situation. (Beware the self-proclaimed instant expert making predictions!) Following the best practices of intelligence analysis is critical in such an uncertain situation. Rather than guessing at the most likely direction of a conflict based on conventional wisdom, a discerning analyst will ask these questions:

1. What are the combatants' stated goals in the conflict, and what are the interests behind those goals? Are they maximalist goals or limited ones?
2. What is the character of the conflict? Is one side roundly condemned as the aggressor? Is either side accused of war crimes, with some compelling evidence to back it up? Are gruesome images of the conflict circulating and suggesting one side is likely to be depicted as malicious, even evil? Are there large-scale civilian deaths?
3. Historically, how committed have these combatants been to achieving their interests? Have they committed blood and treasure to achieve a political end before? What are the institutional and political brakes on them fully committing to achieve this objective today?
4. Does either side see this conflict as an existential threat? What is the minimum level of security required to allow the parties to feel secure enough to stop fighting?
5. What is the likely impact on the parties' economies? What will they need to prosecute this war, and how much is GDP likely to take a hit? Will they be able to export to keep their economy going, or will sanctions too heavily impact their economy?
6. Does either side have powerful outside allies who are willing to fund and supply the war effort? (Outside help tends to make conflicts far longer and stickier.)
7. Critically, what is different about this conflict? (Amateurs are often eager to make comparisons to historical cases, without doing the needed critical thinking on which lessons transfer and which do not. Ukraine has often been compared to World War I, for example, but those analogies rarely hold up.)
8. What is the most likely path forward? What are the left- and right-hand boundaries of likelihood, based on what critical uncertainties? What assumptions are we making about the parties to the conflict? Which of these assumptions could be utterly wrong, and what are the consequences if they are? (For example, many analysts assumed that the Russian army would bowl over the Ukrainian army within a few days. They were very wrong.²)
9. How long is this conflict likely to be in the news? Will it be a long-term issue or fall out of the news cycle quickly? Will it hold public attention? Is there a compelling story behind the conflict, robust media interest, and a steady stream of first-person footage from the

front lines (e.g., Ukraine, Gaza)? Or is it likely to flare and then fade (e.g., Israel-Iran, Yemen, the DRC)?

10. What is U.S. policy on the conflict now? Where is it likely to be in three months? A year? Is the government likely to offer any incentives for supporting U.S. policy or protections for those who choose to assist? Are there indications that a sanctions regime will change because of the conflict? Are secondary sanctions likely to become an issue?

The more entrenched the parties, and the more they view the conflict as existential, the more extended and brutal the fighting is likely to be. Further, observers tend to be overly optimistic about the length of a conflict; rarely is anything ever a “short war.”

Think tanks like CSIS are particularly well positioned to help companies anticipate the likely direction of a conflict. Critical to creating this insight is a combination of deep regional expertise, functional expertise (for example, on the art and practicalities of warfare), and analytical independence. CSIS in particular can draw on a rich network of global contacts to answer questions and build a robust picture of the road ahead.

The more entrenched the parties, and the more they view the conflict as existential, the more extended and brutal the fighting is likely to be. Further, observers tend to be overly optimistic about the length of a conflict; rarely is anything ever a “short war.”

The next section on in-region posture is not conflict-specific, but company-specific. Only you know your exposure inside the combatant countries and what you had planned for the future there.

WHAT IS OUR POSTURE IN THE COMBATANT COUNTRIES?

What is the company's exposure to the conflict? What is the risk to physical assets, intellectual property, and company reputation? Put simply, what do we stand to lose? On the other hand, are there any new demands arising that will allow our business to thrive?

Once you understand the conflict, you need to fully understand your exposure. Pull together key statistics about the company's posture in each country:

1. How many people does your company have in the conflict zone (both expats and local staff)? Where are they? What are their options for evacuation? Are there multiple commercial options? Is the national government offering assistance?
2. What physical assets do you have in country? Where are they? Are any mobile? Which are in an active conflict zone? Which are in a place likely to become an active conflict zone?
3. What information assets or intellectual property do you have in country? Where are they? How robust is their protection? Are there offline backups? Where?
4. What percent of company revenue comes from activity in Country A? In Country B?

- a. What impact is the conflict likely to have on that revenue projection, if your company makes no changes to operations?
 - b. Do you have options for recovering that revenue loss, should you choose to change your operating posture? What level of revenue loss is existential, what level is painful but survivable, and what is impactful but only marginally significant?¹
 - c. Do these answers change if the conflict lasts more than a year? More than three? More than 10?
5. Do you provide essential civilian services in either country? Will ending those services risk civilian lives?
 6. Is it possible to split the business and hive off the elements that are more closely related to defense? Is it possible to expand those activities to support one of the combatants more effectively? What new need has emerged within the country for defense-related help?
 7. If you are a public company, what have your key shareholders said about the conflict? Do you have activist investors who will seek to shape policy?
 8. Are your employees activist? Have influencers in the workforce advocated for a certain policy path?
 9. Is your key customer the public, governments, or other businesses (i.e., B2C, B2G, or B2B)?
 - a. If B2B or B2G, what have those businesses or governments said about the conflict?
 - b. If B2C, does your customer have a ready alternative to your product?
 10. What sanctions have global powers put in place? Do you have the legal resources to navigate the rules effectively?

The answers to these questions will inform everything that follows—from your company’s ability to absorb losses to the potential reputational exposure involved.

Step 2: Discuss the Intangibles

What decision here most closely aligns with our values and reputation? What decisions do we need to make between right and wrong, or even between right and right?

Some questions do not have clear, fact-based answers. Rather, company leadership must make informed judgments and trade-offs between risk and values and between certainty and uncertainty. These are judgment calls, and they deserve careful thought.

1 In the war games conducted by CSIS, participants tended to land at a tipping point of 9 percent of revenue. Less than that was a marginal concern at most; more than that meant real discomfort in making this decision. For more, see Appendix 1.

1. Does your company lead with values? How might those values shape your view of the conflict? How are your shareholders (or stakeholders) likely to interpret your values in the context of the conflict?
2. Is your company an industry leader? Will your decision set the tone for others? Have competitors already made their decisions? Does that set the tone for you, or is there an advantage to be gained in differentiating yourself?
3. What are your competitors doing? How have they positioned themselves in the conflict?

This is a good time to engage deeply with the board to ensure all leadership is on the same page about the company's values and direction.

What decisions do we need to make between right and wrong, or even between right and right?

Step 3: Assess the Risk

Given the likely direction of the conflict and our exposure, how risky is this situation for the company? Is this an existential risk or a minor one?

CSIS constructed a framework for categorizing risk: physical, financial, legal and compliance, and reputational.² These are broad buckets, and some areas overlap—for example, a legal risk becomes a financial risk. A reputational hit affects the financial bottom line. A fumbled response to a physical risk can easily damage a reputation. The risks of cyberattacks or supply chain disruptions—perhaps the most real and present dangers for companies operating in conflict zones—can also fall into both the financial and reputational buckets.

With a full picture of your company's posture, exposure, and values in mind, we can establish the level of risk. Two options below will move step by step through that calculation:

- The first is the analog version. This chart translates open-ended questions into a focused series of yes/no answers.
- The second option is an AI-assisted method. The prompts capitalize on the AI system of your choice to gather and process complex information. This method could uncover potential unforeseen challenges.

2 Cyber risk was factored into several of these categories, including financial and reputational risk, during the war games. Cyberattacks were considered a tool that creates financial or reputational risk, rather than an independent risk. In the worksheets and AI prompts, evaluating cybersecurity posture becomes a core element of identifying exposure to risk.

CHART THE RISK

Check yes or no in the boxes in the chart below. They are designed to be binary answers for the purposes of clarifying the process and your thoughts. While the binary does not capture all the nuances, it forces clarity and decisiveness. More YES answers means higher risk. There are 20 elements; a risk score of more than 15 is extremely high.

Table 1: Assess Specific Risks

Type of Risk	Critical Question	YES	NO	NOTES
Financial	If we shut down in one or both of the conflict countries, is the revenue loss catastrophic?			
All	Is this likely to be a long conflict?			
Reputational	Do we provide essential civilian services?			
Reputational	Do we have activist investors or stakeholders?			
Reputational	Do we have activist employees?			
Reputational	Is our main customer the public/consumers?			
Financial	Do our customers have ready alternatives to our product?			
Physical	Do we have a significant proportion of employees in the conflict zone? ³ Are they expats potentially requiring evacuation?			
Physical	Do we have significant physical assets in the conflict zone? Are they permanent (not movable)?			
Financial	Are our information assets or intellectual property at risk?			

3 “Significant” will mean different things to different companies. In simulations, 10 percent seemed to be a tipping point for participants, but the calculation will vary.

Legal	Is there a robust or convoluted sanctions regime in place? Is it going to require expert advice to navigate?			
Financial	Are we a public company?			
Reputational	Are we out of alignment with our competitors?			
Reputational	Is the story behind the conflict capturing the public imagination? Is there a perceived “bad guy”?			
Reputational	Have there been extensive civilian deaths?			
Reputational	Are we a values-forward company?			
Reputational	Are we an industry leader? Will our decision set the tone for others?			
Reputational	Are we out of alignment with U.S. policy, as we understand it?			
Physical	Has the USG said they will NOT protect businesses involved in the conflict?			
Physical	Is one of the combatants a sophisticated cyber actor, or known for sabotage, assassinations or harassment of opponents, or gray zone operations? ⁴			
	TOTAL			

4 Gray zone operations are tactics that advance larger goals but deliberately hover below the threshold of conventional military activity. They often conceal the hand of the orchestrator or are deniable. The goal is usually to create confusion or destabilize an opponent without triggering a wider conflict. For more, see Seth Jones, “Russia’s Shadow War Against the West,” CSIS, *CSIS Briefs*, March 18, 2026, <https://www.csis.org/analysis/russias-shadow-war-against-west>.

This is not a quiz with one answer. There is no decoder ring. More YES answers means the stakes are higher and the consequences of a decision are real and impactful. The higher the score, the greater the need to plan mitigation strategies. This chart lays out your risk in clear black and white terms. For comparison purposes, CSIS researchers assessed several companies' answers to these questions in the context of 2022 and Russia's full-scale invasion of Ukraine. While CSIS information was incomplete, researchers estimated Starbucks would be at 13, McDonald's at 15, and CrowdStrike at 11.

RISK ASSESSMENT: AI ASSIST

AI's ability to gather and analyze complex data is a powerful ally in this process. The prompt below will drive an exchange with your agent of choice, perhaps uncovering new angles to the questions. It should provide actionable initial feedback, which a leadership team can use to delve further into risks and uncertainties.

A note: Several parts of this prompt will return far better answers if the tool has access to proprietary company data. Ideally, you would run the queries on an internal network.

Prompt: Assume the role of a senior executive at [Company Name]. A conflict has broken out between [Country A] and [Country B]; [both/one] hosts significant company operations. Identify potential risks to [Company Name]. Pay special attention to these six domains: physical, cyber, software supply chain, financial, legal/compliance, and reputational.

Evaluate risk given the below specific architecture, exposure, and business reality.

Note: The analysis will be more specific if your company is willing to educate the AI agent.

Inputs (to be provided by the company)

- Countries involved:
 - Country A (conflict initiator)
 - Country B (conflict victim)
- Nature of company operations in each country (core business lines):
- Revenue exposure (%):
- Employee presence (local/expat):
- Key assets (physical, digital, IP):
- Current sanctions regime:
- Public posture to date (company statements, partnerships, etc.):
- Critical software and infrastructure in use:
- Third-party service providers (if any):
- Key stakeholders (shareholders, customers, governments, etc.):

Risk Mapping

Categorize risks and assess the likelihood and impact of each within the following categories. For each category, evaluate risks over the next [time horizon].

1. Physical Risks

- Damage or disruption to physical infrastructure (e.g., facilities, warehouses)
- Identify secondary impacts (e.g., supply chain disruptions, currency fluctuations)

2. Cyber Risks

- Identify threats to IT infrastructure, including network security, cloud services, and operational technology: Have any known cyber threat actors originating from [Country A] previously targeted [Country B]? If so, identify them by name and describe their past operations (e.g., DDoS attacks, spear-phishing campaigns, exploitation of zero-day vulnerabilities, etc.).
- Source code and dependency risks: Evaluate if the company's software dependencies (open-source, third-party) have known vulnerabilities or unpatched security gaps that could be exploited. Draw on open-source reporting from cybersecurity outlets (e.g., Bleeping Computer, CyberScoop) and major Western news organizations (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News).
- Risk of cyberattacks (e.g., ransomware, data breaches): Quantify the likelihood of disruptive cyberattacks and potential impact using threat assessments from cybersecurity firms (e.g., CrowdStrike, Mandiant), major technology companies (e.g., Microsoft), and official advisories from government agencies (e.g., U.S. CISA, the UK NCSC).

3. Software Supply Chain Risks

- Audit the source code, third-party libraries, and open-source packages for known vulnerabilities or missing critical patches.
- Assess the risk of compromised or tampered dependencies in the development pipeline (e.g., via supply chain attacks).
- Evaluate the security posture of [Company's] software providers. Do any of them have a history of breaches or known vulnerabilities?
- Identify redundant systems or fallback mechanisms in case of service interruptions. Where do we lack redundancies in critical areas?

4. Financial Risks

- The current sanctions picture is [fill in details]. Given past U.S. policies during this type of conflict, what type of sanctions do you anticipate will be forthcoming in the next six months of this conflict?
- Given that answer, assess the impact of those expected sanctions on revenue and operations.

5. Legal and Compliance Risks

- Identify areas where our company's operations could run afoul of sanctions regimes, including secondary sanctions from the U.S. or allied countries.
- Evaluate potential legal actions against the company (e.g., lawsuits related to alleged complicity in war crimes, genocide, or human rights abuses, and lawsuits related to breach of contract). Draw on DOJ indictments and official press releases, and UNHCR reports from previous, similar conflicts.
- Consider local laws that might change rapidly during conflict and could affect operations or employee safety (e.g., martial law, rule by decree, nationalized assets).

6. Reputational Risks

- Assess how the conflict is likely to affect the company's public image and brand perception. How might our actions in this conflict contravene our public statements and company values?
- Consider activism within the company, including employees or stakeholders publicly demanding action. Determine when employees have publicly protested company actions or issued open letters to management, and assess the outcomes of these activities. Draw on reporting from major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News).
- Identify potential media narratives that could emerge and damage public trust, such as accusations of unfair business practices, participation in unethical activity, corruption, or exploiting the conflict for profit.
- Assess whether the company is perceived as a neutral party, or if its operations could be seen as directly contributing to the conflict. Draw on official statements from both countries' governments to assess whether (and how) they have publicly referenced the company since the outbreak of the conflict.

Recommendations for Immediate Action

Provide immediate actionable steps to address high-priority vulnerabilities, such as:

- Initiating vulnerability scans for source code and critical infrastructure
- Deploying emergency patch management for known threats
- Engaging with external security experts to address gaps in software dependencies
- Updating contingency plans to reflect the latest risk assessment

Step 4: Make an Initial Decision

We find ourselves unexpectedly on the front lines of conflict. What will position the company best through this crisis? How can we minimize risk, take advantage of potential upside, and take care of our people and our customers?

The above exercise should illuminate a strategy in alignment with company values. Now, fully explore the implications of that path. Make a preliminary decision. Then, stress-test it by unraveling the potential consequences.

The following section lays out six options for a decision on engagement or disengagement in the affected region. These are illustrative, not comprehensive; they arose out of the series of war games with industry leaders. A mix of a couple answers might be the right path for your company. Each option includes questions that will help check the practicality of that path forward. Broadly, those options are to stay in both combatant countries, partially wind down operations, segregate the defense-heavy business into a local subsidiary, or cease operations in one or both combatant countries.

DECISION OPTION 1: STAY IN THE CONFLICT ZONE

Perhaps the assessment is that the war will be more a skirmish than a drawn-out conflict, like so many exchanges of fire along the India-Pakistan border, for example. Perhaps the fighting is highly localized and operations in-country are too important to your company's business model. Maybe there are good values-based reasons to maintain operations as-is. Staying put may be the best option.

- Protection of people becomes paramount. Do we have a feasible employee evacuation plan? What is our "trip line" for evacuating? How can we reduce our presence to as few staff as possible? Can we evacuate families now?
- How are the combatant countries likely to view our operations? Can we expect help from either side, or are they going to view us as a potential target?
- Of our in-country assets, which are most at risk, and from what?

DECISION OPTION 2: PARTIAL WIND-DOWN OF OPERATIONS

Drawing down to minimal staff and limited operations is a halfway measure that has served governments well in times of crisis. Every U.S. embassy has a contingency plan to operate with a skeleton crew of essential staff. Perhaps your company has the time and resources to wait and see with a greatly minimized posture.

- How long is a skeleton crew posture sustainable?
- How can we reallocate people and resources? Which assets are movable and which must be abandoned?
- Can the company temporarily move staff to neighboring countries? What will be the cost, and will those staff get caught up in a massive refugee flow?

DECISION OPTION 3: SEGREGATE DEFENSE-RELATED ACTIVITIES OR ESTABLISH A LOCAL SUBSIDIARY

One approach to reducing corporate risk while providing conflict assistance is to segregate elements of the company conducting defense-adjacent activities from those performing strictly civilian functions. Business splitting, holding companies that house various subsidiaries (think

Google, a subsidiary of Alphabet Inc.), and industry conglomerates are common features of the modern corporate landscape. The establishment of a locally owned enterprise, wholly distinct from any existing corporate structure, may be necessary to balance conflict support priorities with fiduciary duties.

- Can we segregate our defense-adjacent work from our other work, or does that require too much duplicating of processes and equipment?
- Does splitting the company actually minimize the risk profile? Are the combatants likely to see the civilian parts of the business as less of a target if we hive off the defense portion?

DECISION OPTION 4: EVACUATE AND SHUT DOWN IN COUNTRY A

For the purposes of this paper and the war games CSIS ran, “Country A” was the aggressor country that, much like Russia, invaded a neighbor without provocation. For this option, a company might do what so many did at the start of the full-scale invasion and pull out of the aggressor nation. This avoided messy sanctions, aligned companies with the values of democracy and peace, and—for most—caused minimal losses to the business, given an already minimal presence in Russia. But it also made companies more of a target for an angry Kremlin. Conversely, many businesses not only stayed in Ukraine, but leaned in heavily to assisting Kyiv with its efforts to withstand the Russian full-scale invasion. Cybersecurity companies in particular were essential to defending Ukraine from massive Russian cyberattacks, but banks and tech companies were also among the hundreds who stayed to help.

- Does making a judgment call on good actors and bad actors align with our company values?
- Do we provide essential civilian services in Country A that will be lifesaving in time of war?
- Can we move people out quickly and safely?
- Can we prevent the host country from capturing and repurposing our assets for their own use?

Many businesses not only stayed in Ukraine, but leaned in heavily to assisting Kyiv with its efforts to withstand the Russian full-scale invasion. Cybersecurity companies in particular were essential to defending Ukraine from massive Russian cyberattacks, but banks and tech companies were also among the hundreds who stayed to help.

DECISION OPTION 5: EVACUATE AND SHUT DOWN IN COUNTRY B

What if the fighting in the victim country is too intense to sustain business operations? When ISIS attempted to establish its caliphate in 2014, it engaged in brutal assaults on civilians and combatants alike. No one was safe, and its forces rolled forward faster than anticipated. Attempting to operate in such an environment is too dangerous for any business.

- Can we move people out quickly and safely?
- Can we prevent the aggressors from capturing and repurposing our assets for nefarious ends?

DECISION OPTION 6: EVACUATE AND SHUT DOWN IN BOTH COMBATANT COUNTRIES

Perhaps the fight looks like it will be long and cause widespread destruction, and perhaps both countries are committing horrific acts of violence against civilians. On balance, the benefits of continuing to operate might be minimal in comparison to the risk to staff, assets, and reputation.

- How big a financial hit will pulling out of the conflict region be for the company? What durable assets are we going to have to leave behind?
- What happens to our local staff in both countries? Can we relocate or reallocate them?

AI ASSIST: DECISION TESTING

Evaluate how these risks might change based on our decision to [stay in the conflict zone / partially wind down operations / segregate defense-related business / pull out of Country A / pull out of Country B / pull out of both countries]. Specifically:

- Does reputational risk worsen if we pull out of [Country B, or the “victim” country]?
- Does physical risk worsen if we only pull out of [Country A, or the “aggressor” country]?
- Do risks significantly improve if we segregate defense-related from civilian parts of the business? If we create a local subsidiary to manage defense-related business?

Step 5: Develop and Stress-Test Mitigation Strategies

Some level of risk is inevitable, so now what? If we carry out our preferred decision, what can we do to mitigate the risk? How can we insulate ourselves against a potentially catastrophic outcome?

You’ve decided on your preferred course of action—a plan that aligns best with your values, goals, the law, and company policy. But no matter what the decision, there will continue to be risk as long as the conflict continues. How can you mitigate these risks?

To structure the mitigation strategies, it is most helpful to return to the risk framework: physical, financial, legal and compliance, and reputational. Given your preferred course of action, what steps are possible in each category to minimize downside and create potential upside? The below list is illustrative—your business will have its own concerns, opportunities, and capabilities.

Mitigating Physical Risk

- Move assets if necessary. If they must stay in-country, look for coverage from national air defense capabilities and access to multiple transportation routes for evacuation purposes.
- Create shelter protocols and evacuation plans with multiple route redundancy. Ensure you have a good security team with local knowledge. Sign up for real-time alert systems (air raid

apps, local intelligence feeds) and have personnel assigned to monitoring the feeds and sharing information with the team. Designate representatives responsible for liaising with local authorities; make those contacts early and work to maintain strong relationships with the right government officials.

- Understand your insurance coverage. Most policies do not cover acts of war, but much is still unsettled law on what counts in that category, particularly in the cyber domain. Do you have war-risk riders? Will insurance cover emergency evacuation of wounded personnel?
- Install backup power infrastructure (generators, battery systems) for critical systems, given that attacks on energy systems are likely. Consider securing emergency water supplies.

Mitigating Financial Risk

- Maintain liquidity buffers for emergency expenses. Diversify banking relationships, especially locally.
- Look for opportunities to shift a product line to meet the changing demand of a society at war.
- Evaluate what assets you have that may be newly useful, like the geographic and political knowledge of your local staff.

Mitigating Legal and Compliance Risk

- Contract or hire additional specialists for dedicated sanctions compliance review.
- Track martial law legal changes. Governments at war can make new laws and regulations with little warning. A dedicated team can monitor new developments. Local expertise is ideal. AI agents can help scan for new developments and flag potential issues.

Mitigating Reputational Risk

- Craft a communications plan. What is the right message to send to your customers, investors, and stakeholders? How should you reassure them and message how you are aligning the company's values to its decisionmaking?
- Track actions of partner companies and competitors.

Other Considerations

- Create a standing crisis committee that should meet on a fixed cadence, with surge capacity defined for active crisis periods. Work together to exercise contingency plans; iterate on those plans to eliminate points of friction or uncertainty.
- Identify clear authority. Who can authorize evacuation or shutdown without full board sign-off? Where can those authorities be delegated to create redundancies, if someone is unreachable?
- Define trigger points for escalation (e.g., "if the front line moves within X km, execute relocation plan B"). Some entities use the PACE system for levels of planning, which calls for primary, alternate, contingency, and emergency protocols. Notably, each successive PACE option is less ideal but increasingly urgent and simpler to execute.³

- Coordinate with the U.S. government. Who is the best point of contact inside the USG? What level of support are you asking for? Can you get timely, actionable intelligence briefings to help evaluate risk? Are you in alignment with U.S. policy and how will you know if U.S. policy is moving?

AI ASSIST: RISK MITIGATION STRATEGIES

Your preferred AI algorithm can also help construct a risk mitigation strategy tailored to your business. The prompts below are a continuation of the prompts from Step 3: Establish the Risk Level. (The complete set of prompts is also in Appendix 4.)

Risk Mitigation Strategies

Based on this risk evaluation, suggest mitigation strategies for these risks. Prioritize protection of company staff, including executive protection, diversification of critical supply networks, and narratives designed to ameliorate reputational risk.

Physical Risks

- Draft an employee evacuation plan (time frames, triggers, and external support from governments or NGOs). Has the company previously had to evacuate employees? If so, what did that plan entail, and how long did it take to execute? Draw on reporting from major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News) and official company statements.
- Write location-based risk assessments for key infrastructure and staff. Are there specific regions within either country that present higher risk (e.g., proximity to military targets, densely populated urban areas, or strategic locations such as major ports servicing military vessels)? Draw on major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News) and analysis from security-focused think tanks (e.g., ISW and CSIS) on each country's military capabilities, force posture, and potential targets.
- Create contingency plans for reducing company footprint in high-risk zones.

Cyber and Software Risks

- Suggest a vulnerability management process for both internal code and external dependencies, with a focus on immediate patching and redundant systems.
- Suggest a schedule for accelerated audits of third-party dependencies and an implementation plan for dependency isolation to limit exposure to vulnerable or compromised packages.
- Construct a plan for implementing Zero Trust frameworks or network segmentation to reduce overall attack surface.

Financial Risks

- Suggest several options for diversification of revenue streams in case the conflict leads to significant market or region loss.

- Suggest several alternative currency and asset options to protect against exchange rate fluctuations.
- Suggest talking points for discussion with legal counsel to anticipate potential penalties from sanctions. Suggest what questions we should ask our legal counsel.

Legal and Compliance Risks

- Develop an ongoing monitoring system to track changes in both international laws and local regulations.
- Suggest a schedule for us to regularly engage with compliance officers to ensure adherence to sanctions and humanitarian laws.

Reputational Risks

- Suggest a public communication strategy to clearly outline the company's stance in the conflict, balancing values with business continuity.
- Suggest standard operating procedures for spokespeople and legal teams to handle media inquiries and employee dissent regarding the company's position. Where could the company redirect backup resources and personnel to ensure this team remains adequately staffed?

Red Teaming and Stress Testing

Adversary Perspective

Use the results of the above analysis to stress-test the company's preferred risk mitigation strategy by adopting the perspective of external adversaries (e.g., cyberattacks, reputational backlash, legal penalties). [INSERT PREFERRED RISK MITIGATION STRATEGY HERE]

- Consider exploitative tactics used by adversaries (e.g., cyberattacks targeting critical infrastructure, phishing schemes aimed at employees) or public relations campaigns that could amplify negative sentiment.
- Propose adaptive strategies to counteract these potential attacks, with a focus on cyber defense and PR crisis management.

Board Member Perspective

You are now a board member of [Company] with expertise in physical and cybersecurity. Evaluate [Company Name]'s proposed course of action and contingency plan. Identify potential gaps in the proposal, with particular focus on security vulnerabilities to physical infrastructure protection and points of failure on our networks, as well as financial health and reputational effects. This should include assessments of both direct and cascading risks that could arise from unresolved issues in any of the categories.

Final Output

Provide a detailed risk evaluation report categorized by severity, likelihood, and strategic impact, alongside tailored mitigation and contingency recommendations to help the company make informed, timely decisions in this complex and evolving environment.

The Government Stakeholders

A Memo to the President About Supporting U.S. Companies

Industry is only one side of the picture. Government needs to take into consideration the role industry plays, and industry should be sensitive to the government's strategic direction, or at least react to tactical shifts. The below memo to the president aims to bridge the gap, asking the president to take into account the way business must think about its role in global conflict.

TO: The President
FROM: The National Security Advisor
RE: Supporting U.S. Companies in a Conflict with No Front Lines

Several U.S. companies are reassessing their position relative to the conflict between [countries A and B]. Many are not defense companies per se, but are companies that find themselves involved in the war effort. In other words, the concept of “front lines” has shifted to the point of irrelevance. Companies and noncombatants alike are involved.

While our industry partners are eager to align with U.S. policy, they have questions about what support they should expect from the White House and larger U.S. government, particularly if [Country A] treats them as a combatant. They have concerns about the safety of their in-country employees, but they are also deeply worried that their global backbones might be at risk and that their C-suite staff could become targets for assassination. **They are seeking some sign of explicit support from the USG.**

As we debate our approach, some critical considerations:

1. **Resource constraints.** We are a global superpower, but we still have constraints. We are selling arms to help [Country B] defend itself, while working to make peace in regional conflicts and deter other great powers from working to destabilize U.S. global leadership. If we set a precedent of attempting to defend every U.S. company worldwide from any form of attack, we will quickly progress from stable to stretched to unable to follow through on our threats. Where do we draw the line?
2. **Which companies deserve protection?** There are hundreds of U.S. companies with some presence in the current conflict zone, some small and some large. Some play a central role in the defense of the victim; others provide niche services. Should they all expect the same level of protection, no matter their size and role? If not, how should we differentiate?
3. **Escalation to direct conflict.** Defending U.S. companies could spark direct retaliation against the United States. Further, the aggressor may not have intended to strike a U.S. company or U.S. territory; for example, a cyberattack meant to stay in the conflict zone could spill into U.S.-based infrastructure, leading to disastrous consequences.
4. **The critical role of companies in supporting the combatants.** Withdrawal of several companies would leave [Country B] far less capable of fighting. U.S. tech companies have been critical to defending [Country B's] networks and providing backup communications for military and civilian services alike. Several U.S. companies provide food and transportation services, not only for civilians but for the front lines as well. Should they feel abandoned, they might abandon [Country B].

In the current conflict, there is a clear aggressor nation and a clear victim. Nearly all countries have lined up to support the victim, including many of our close allies that also host important nodes for U.S. companies. While we have made clear to both combatants that we will not directly engage in the fighting, our policy is to provide robust lethal and nonlethal support to the victim and to pressure the aggressor to end its invasion with economic and diplomatic pressure.

In this circumstance, we must focus on how best to achieve U.S. goals, which are ending the aggression, halting the bloodshed, and ensuring that the aggressor pays a significant cost for its actions, deterring it from engaging in further adventurism against U.S. allies.

Given those goals, and the vital role some U.S. companies play in shoring up the defensive position of the victim, **we recommend the United States make a declaratory statement of policy: An attack on a U.S. company will be considered an attack on U.S. interests, and we will retaliate in a way and at a time of our choosing. Should the attack on the U.S. company affect assets inside the U.S. homeland, our retaliation will be swift and extensive.** An attack on the homeland is a clear violation of sovereignty and threatens U.S. citizens who are not parties to the conflict.

The threatened retaliation for attacks in country should be intentionally ambiguous to provide flexibility on an appropriate level of punishment. (A direct missile strike on a large U.S. company

compound killing civilians is different than a DDoS attack on a three-person U.S. company operating in country. A destructive cyberattack on a server farm outside of Washington is different as well. Each merits a different, appropriate response.) Our goal for this policy is additional deterrence and reassuring U.S. businesses.

Looking ahead, this approach is best for this conflict, in part because the moral lines are clear. Put simply, there is a bad guy in this moment. However, that may not always be true. **This policy should be stated as the policy for this conflict, not a new doctrine the United States will follow for every conflict worldwide.** Economic or long-running border disputes that escalate into bigger conflicts do not necessarily merit the same level of U.S. investment in a particular outcome. Further, in some conflicts, companies' interests and U.S. interests may be out of alignment. We do not wish to be responsible for a company that chooses to contravene U.S. policy for financial gain.

The concepts of front lines and parties to a conflict are rapidly changing as the conduct of war shifts. Companies that provide nonlethal dual-use services will increasingly find themselves indispensable to a war effort, yet unprepared for what that means. We should also consider an outreach and education mission to critical industry partners to discuss risk and the details of protection we can offer. Partnering with congressional leaders and letting them own discussions with their constituents would be helpful.

Conclusion

Modern war is shifting dramatically in ways that draw in nondefense companies. Data is the new essential edge in conflict. Cloud access is critical to communication, planning, evaluating, and coordinating. Private drone manufacturers, private communications companies, battery manufacturers, and the space industry all find themselves in essence on the front lines of warfare. Further, actors like Russia have always conducted hybrid warfare, including sabotage and assassination of leaders far from the literal front lines. This trend is escalating, with threats to CEOs, attacks on shipping companies across Europe, and mysterious fires at warehouses. Companies that never considered themselves “defense companies” are now surprised to find themselves targets. We cannot think any more about a bifurcation between a combatant sitting on a front line and a support function far from the front. The front lines have disappeared as a concept. Companies find themselves in a world of No Front Lines.

Appendix 1

Gaming Out the New Reality of War

CSIS ran six war games with business and government leaders to gather data on the essentials of decisionmaking in a realistic crisis scenario. CSIS asked these leaders what information they would need during a conflict scenario in order to evaluate physical, financial, reputational, and legal risks and rewards. Each exercise concluded with a decision point: Should their company take a side in the conflict? Researchers gained valuable insights as participants wrestled with both factual and moral dilemmas, including confronting the challenge of managing an impetuous, activist CEO.

In the war game, participants served as advisers to the CEO of “XYZ,” a U.S. technology firm that has business interests in cloud services, cybersecurity, satellite communications, and smart logistics. The company operates in two countries on the continent of Terranova: Bishkova and Albertova. XYZ expects its investments on Terranova to be a major source of future revenue, and existing operations in both countries are already major income streams.

Just before the simulation began, Albertova launched an unprovoked act of aggression against Bishkova, seizing territory and attacking critical economic infrastructure with cyberattacks, drones, and cruise missiles.

In round one of the game, participants received simple fact patterns about the conflict and their company and had to evaluate the risk to the firm. They then had to make a recommendation to the CEO: stay in both countries, leave one country, leave both countries, or craft a halfway measure, like shutting down or spinning off certain business lines. In round two, the company’s highly activist

CEO unexpectedly announces in a social media post that he will fully support Bishkova (the invaded country). Participants were then asked to come up with a mitigation plan.

CSIS researchers found participants to be overly optimistic that they would not be considered a part of the military effort. Shifting this mindset will be crucial to positioning a company for success in a conflict scenario.

The most striking takeaway from the exercise was how sharply divided participants were on nearly every issue. One source of intense debate was whether the combatants would consider their company a party to the conflict, and thus a legitimate target. This was hugely important in evaluating risk, and CSIS researchers found participants to be overly optimistic that they would not be considered a part of the military effort. Shifting this mindset will be crucial to positioning a company for success in a conflict scenario.

Findings

Key findings from the exercises include the following:

- Participants were highly divided on whether the company was a direct participant in the conflict (41 percent no; 38 percent yes), meaning participants overall were unsure whether their assets or employees would be considered legitimate targets.¹
- Participants lacked consensus on which types of services might make a company more likely to be considered a combatant. When asked which service or services (participants could pick more than one) could tip the balance, a plurality of players identified smart logistics (35 percent), while similar shares pointed to satellite communications (27 percent) and cyber services (24 percent) on top of the list. Only 14 percent said cloud.
- In the end, nearly half (49 percent) of the participants decided to keep doing business in both warring nations. Another 39 percent opted to support only Bishkova (the “victim” side of the conflict), while 9 percent decided to withdraw from both markets.
- Participants also noted that additional details about the company—such as the political activity of its employees and CEO and the nature of its business partnerships—might have influenced their decisions. Participants said that a company’s response likely would depend on the level of political activism of its employees, or, as one participant put it, “how much your employees revolt.” In 2024, Google terminated 28 employees who participated in protests against the company’s cloud contract with the Israeli government amid Israel’s war

1 The numbers do not add up to 100 because the remaining 21 percent did not see the question; in later iterations of the game, researchers made sure to prompt participants to answer that question.

in Gaza.⁴ Google absorbed the reputational hit, but smaller companies might not have the same resilience and could be more inclined to align their activity with employee sentiment.

- The amount and tone of media coverage surrounding the conflict would shape whether a company chooses to remain or withdraw, especially for consumer-facing companies that are sensitive to public perception. (See the section below on reputational risk for more on this.)
- Participants also emphasized that if the U.S. government were to issue an official statement amid the conflict supporting or condemning one of the warring nations, the company would likely need to align its actions accordingly.
- There was a general consensus across iterations of the game that the decisions needed to include a variety of perspectives. At the very least, the company's security, legal counsel, and board members should be in the room. Other top responses included the communications team, business operations, and human resources.
- Industry leaders demonstrated limited understanding of how to engage with the U.S. government for information or assistance during a conflict. Nearly half identified the White House (48 percent) as their first choice—a choice that may be feasible for large or prominent companies but less so for smaller entities. Participants pointed to NSA (16 percent), CIA (10 percent), FBI (10 percent), and State Department (10 percent) as other top agencies to contact.
- Regardless of who they planned to contact, participants had depressingly low expectations for the quality of support they expected from the U.S. government. At most, they hoped to understand and stay in alignment with U.S. policy. When researchers suggested the government might provide additional support, like statements intended to deter the parties in the conflict from attacking companies, they were beyond skeptical but said that kind of support would make a huge difference.

THE RISKS

Participants hotly debated the potential physical, financial, legal/compliance, and reputational risk associated with being perceived as involved in a conflict. They discussed which risks would be the most likely to occur, which would be the most damaging or impactful, and what steps could best mitigate each risk.

Across all categories, participants indicated that a company's size and public profile would affect the likelihood and impact of each risk. Whereas a small company can "fly under the radar," an industry leader would likely face far more scrutiny for its decisions. Extensive media coverage of a conflict exacerbates the problem, particularly for consumer-facing companies that are more exposed to public opinion.

The chart below describes participants' combined evaluation of the likelihood that a category of risk would affect a company and the impact of that risk if it were to come to pass. The lower the number, the more critical the risk.

Table A-1: Scoring Risk Across Categories

Risk Category	Average Likelihood Score ²	Average Impact Score	Meaning
Physical	2	2	Likely; critical impact
Financial	3	3	Chances are even; moderate impact
Reputational	2	3	Likely; moderate impact
Legal	3	3	Chances are even; moderate impact

Likelihood Scale: 1= very likely, 2= likely, 3= chances are even, 4= unlikely, 5= very unlikely.

Impact Scale: 1= catastrophic, 2= critical, 3= moderate, 4= marginal, 5= negligible.

Physical Risk

Participants unanimously prioritized the physical safety of their people as the company's foremost objective at the onset of the conflict. They ranked physical risk as both likely and critically impactful, emphasizing that protecting personnel should be at the center of the company's decisionmaking. As one participant put it, "Your first job is to protect your employees and then to protect your infrastructure." In addition to direct threats to staff and facilities, participants also considered what one described as "incidental physical risks." For example, disruptions to a country's grid, water, or other critical services could severely limit a company's ability to work and may ultimately force it to withdraw from one or both countries.

Financial Risk

Game participants generally saw financial risks as both less likely and less impactful than physical risks, rating them as moderate probability/moderate impact. Within this category, they highlighted sanctions and public boycotts as the most significant financial risks. For instance, if sanctions were imposed on one of the actors, the company would face substantial financial losses. As one participant put it, "If it's a large market or large supplier [for the company] that can really change things. Compliance costs are going way up."

Participants also noted that public boycotts can severely affect the company's bottom line, particularly for public-facing companies, and financial risks are more pronounced in conflicts receiving extensive media coverage. For example, since Russia's full-scale invasion of Ukraine, the Yale School of Management reported that over 1,000 companies publicly announced that they curtailed operations in Russia, likely anticipating public opinion on the conflict.⁵ With Israel, activists have encouraged consumers to boycott brands perceived as supporting the country. For example, Starbucks reported slower sales in the first month of 2024 due to decreased business in the Middle East.⁶ McDonald's similarly reported slower sales, particularly in the Middle East and Muslim majority nations, which it also attributed to the conflict in the Middle East.

2 Both average likelihood and average impact are rounded to the nearest whole number.

Reputational Risk

Participants viewed reputational risk as very likely but only moderately impactful. They emphasized that companies with a strict moral code or statement of values should use these principles to guide decisions about where to operate and which services to provide. As one participant noted, acting contrary to the company's moral code could upset shareholders or employees or even provoke public boycotts. Patagonia, for example, openly publicized support for Ukraine, acting in alignment with its environmental focus by highlighting the interconnectedness of the conflict with the global climate and energy emergencies.⁷ Additionally, companies must consider whether discontinuing services would harm civilians who rely on them for survival. In such cases, stopping operations could bring negative reputational consequences.

Legal Risk

Finally, participants assessed legal risk as moderate likelihood and moderate impact. These risks include lawsuits or complaints related to international humanitarian law, violations of U.S. sanctions regimes, or lawsuits initiated by local stakeholders or NGOs. For example, in June 2025, the French League for the Defense of Human Rights sued arms producer Eurolinks for suspected acts of “complicity in war crimes,” “complicity in crimes against humanity,” and “complicity in the crime of genocide.”⁸ Likewise, in November 2024, Ben & Jerry's sued its parent company, Unilever, for silencing its activism in protesting the war in Gaza and criticizing Donald Trump.⁹ A participant noted that, depending on the situation, these legal costs combined with the physical risks may eventually exceed the financial loss of discontinuing services.

Appendix 2

Case Study on Microsoft in Ukraine

The first response of a business when a war breaks out is typically to leave the battle and get as far away as possible. And yet if we're going to do what we strive to do in our mission as a company, which is to provide the infrastructure on which everyone relies, it needs to protect countries in times of war *and* in times of peace.

-Brad Smith, Microsoft Vice Chair and President, interview with the *Washington Post*, June 23, 2022¹⁰

Microsoft has played a critical role in helping Kyiv defend against Russian cyberattacks, detecting new malware packages such as FoxBlade and working closely with Ukrainian cyber defenders to protect key systems.¹¹ Since the start of the war, Microsoft has continued to provide defensive support and threat intelligence while helping the Ukrainian government migrate data to the cloud, relocate servers outside the country, and automate the protection of large-scale networks. For example, the company committed \$107 million to shift government data and computing infrastructure to the cloud.¹²

This case study examines the key decisions Microsoft has made since the invasion began. While researchers do not have direct insight into internal executive deliberations, the timeline is drawn from official Microsoft statements, public interviews with company leadership, quarterly earnings calls, and news reporting to trace the company's decisions from March 2022 to May 2025.

Eight days after the full-scale invasion, on March 4, 2022, Microsoft announced that it would “suspend all new sales of Microsoft products and services in Russia,” while continuing to

support existing customers.¹³ The company stated that the decision was taken “in lockstep with the governments of the United States, the European Union and the United Kingdom and . . . in compliance with governmental sanctions decisions.”¹⁴ Immediately after the announcement, Microsoft’s share price fell by 2 percent, erasing \$40 billion in market capitalization and wiping out most of its share-price gains since the start of Russia’s full-scale invasion of Ukraine.¹⁵

On June 8, Microsoft further announced that it was “significantly [scaling] down [its] operations in Russia” in response to “changes [in] economic outlook” and the ongoing impact on its business.¹⁶ As part of this move, Microsoft announced that it would lay off nearly 400 employees based in Russia.¹⁷

Later, on June 23, 2022, Microsoft Vice Chair and President Brad Smith gave an in-depth interview with the Washington Post to elaborate on the company’s decision to help Ukraine and withdraw from Russia.¹⁸ When asked how Microsoft decides which countries to assist, and whether it would have aided Russia had Ukraine attacked first, Smith explained that, in recent years, the company has “started thinking about [its] responsibility [to individuals, businesses, and entire nations] and what it meant in a more robust way” and ultimately “developed a set of principles.” The first of these principles, he mentioned, is that Microsoft “has a responsibility to *defend* countries” (emphasis his). He clarified that while Microsoft “won’t help governments attack others, especially innocent civilians,” it does view itself as having this “defensive responsibility.”¹⁹

Smith later maintained that Microsoft’s responsibility in Ukraine “is not a difficult one,” describing the country as a “democratically elected country that is being unjustly [and] unlawfully invaded by Russia acting as a hostile aggressor.” He further noted that Microsoft’s approach aligns with the principles of the Geneva Conventions, which emphasize the protection of civilians on both sides of a conflict. Smith noted that Microsoft “has been consistent with those principles,” and explained that the company “will not be taking away [its] downloads for hospitals in Russia or medical clinics.” While Smith acknowledged that Microsoft is operating in largely uncharted territory, he concluded that the company’s role is “grounded fundamentally in the role it plays for the United States, for the democracies of the world [and] for NATO, but also as a defensive protector, especially for innocent civilians around the world.”²⁰

When asked about Microsoft’s prominent role in defending Ukraine against cyberattacks, Smith explained that because cyberspace is “owned . . . operated, and . . . protected, in part by the private sector [and], in part, by tech companies,” Microsoft’s role is “not only indispensable, but unavoidable.” Although he acknowledged that “the first response of a business when a war breaks out is typically to leave the battle and get as far away as possible,” he argued that, if Microsoft is to fulfill “its mission as a company,” which is to “provide the infrastructure on which everyone relies,” it must protect countries “in times of war *and* in times of peace” (emphasis his). He went on to say that the war in Ukraine is “not just a war between Russia and Ukraine,” but one that also involves “an alliance of countries supporting Ukraine and an alliance of tech companies.”²¹

When asked about Microsoft’s continued operations in Russia, despite having significantly scaled them down, and whether the company is taking special measures to protect its remaining employees there, Smith explained that Microsoft, like many other firms, is “seeing its business [in

Russia] narrow and narrow and narrow until eventually there's barely or maybe nothing there." He added, however, that Microsoft remains committed to supporting its employees in Russia, emphasizing that the company is doing its best to "provide them with the kind of support they need and deserve." He did not, however, elaborate on what this support would look like.²²

Microsoft's decision to withdraw from Russia had a noticeable impact on its bottom line. During its July 26, 2022, fourth-quarter earnings call, Microsoft Chief Financial Officer Amy Hood partially attributed the company's lower-than-expected earnings to Russia's war against Ukraine, noting that Microsoft had spent \$126 million to "scale down" its operations in Russia. She also announced that, during the same quarter, the company had incurred \$113 million in employee severance costs—a figure that excluded Russia, where the total would have been even higher. As an immediate result of the earnings call, Microsoft's stock dipped 1 percent in after-hours trading.²³ This Q4 earnings call was the only time Microsoft referenced Russia and the conflict in Ukraine, and it made no such mention in any subsequent earnings calls.

On June 21, 2022, Western media reported that Microsoft was restricting Windows 11 updates for existing Russian users.²⁴ Although Microsoft did not issue an official announcement, these claims were later verified by cybersecurity news company BleepingComputer, which used a VPN server based in Russia to confirm that Microsoft had, in fact, disabled Windows 10 and Windows 11 updates in Russia.²⁵

In August 2023, Microsoft officially announced that it would stop renewing software licenses for Russian companies, effective September 30, 2023. According to Nikolai Komlev, director of the Russian Association of Computer Technology Manufacturers, this phased approach was intended to give customers time "to transfer data and make backup copies."²⁶

Two years after the full-scale invasion, on March 15, 2024, Microsoft announced that it would suspend software and cloud services for Russian customers.²⁷ Users were given several days (until March 20) to collect and preserve their data before the suspension took effect.²⁸ The company reportedly shut down 50 cloud services by March 23, according to Western tech journalists.²⁹

On May 26, 2025, President Vladimir Putin announced that foreign companies acting "against Russian interests," including Microsoft and Zoom, should be "throttled" in Russia.³⁰ Shortly thereafter, on May 30, 2025, Microsoft's primary legal entity operating in Russia officially filed for bankruptcy.³¹ Microsoft in essence implemented a phased approach to winding down its services—first banning the purchase of new licenses, then restricting software updates, and ultimately suspending cloud and software services.

Appendix 3

Case Study on Attacks on Data Centers in the Iran War

In the early stages of the Gulf conflict, Iran made a deliberate strategic choice to declare commercial cloud infrastructure a legitimate military target. Iranian drone attacks in early March hit two AWS data centers in the United Arab Emirates and one in Bahrain, causing moderate physical damage but widespread service disruption—banking systems, consumer platforms, and communications suffered service interruptions across the region.

Then, on March 11, an actor that was likely Israel struck a Bank Sepah data center in Tehran—one containing payroll records for the IRGC and the Iranian army. The strike disrupted banking and salary payments to Iranian military personnel.

They are, in the end, companies—and they are being asked to carry risks that companies were never designed to bear alone.

That same day, an IRGC-affiliated news outlet published a list of 29 “tech targets” Iran planned to strike across Bahrain, Israel, Qatar, and the United Arab Emirates. The list named facilities belonging to AWS, Microsoft, IBM, Google, Palantir, Nvidia, and Oracle—all U.S. companies, and all designated as “legitimate targets” on account of their purported ties to Israel and U.S. military operations.³²

Iran has now made explicit that it views U.S. tech infrastructure as a legitimate theater of attack. This creates a structural problem. Data centers cannot be relocated the way data itself can. Tech

companies employ security professionals and intelligence analysts, but they do not have armies or air defenses. They operate without access to the \$80 billion intelligence apparatus the U.S. government deploys in support of national security. They are, in the end, companies—and they are being asked to carry risks that companies were never designed to bear alone.

Tech companies will face a difficult calculus: The risks of operating near conflict zones may outweigh the returns. If major firms begin scaling back their exposure in risky geostrategic neighborhoods, the consequences will extend well beyond commerce. The warfighter would lose the data infrastructure, cloud computing, and AI capabilities that modern operations depend on. The United States would lose the most powerful force multiplier it has developed in a generation.

Appendix 4

Complete AI Prompt

Risk Assessment: AI Assist

AI's ability to gather and analyze complex data makes it a powerful ally in parsing these decisions. The prompt below will drive an exchange with your agent of choice, perhaps uncovering new angles to the questions. It should provide actionable initial feedback, which a leadership team can use to delve further into risks and uncertainties.

A note: Several parts of this prompt will return far better answers if the tool has access to proprietary company data. Ideally, you would run the queries on an internal network.

Below is the entire AI prompt, ready to paste into your agent of choice.

Step 1

Prompt: Assume the role of a senior executive at [Company Name]. A conflict has broken out between [Country A] and [Country B]; [both/one] hosts significant company operations. Identify potential risks to [Company Name]. Pay special attention to these six domains: physical, cyber, software supply chain, financial, legal/compliance, and reputational.

Evaluate risk given the below specific architecture, exposure, and business reality.

Note: The analysis will be more specific if your company is willing to educate the AI agent.

INPUTS (TO BE PROVIDED BY THE COMPANY)

- Countries involved:
 - Country A (conflict initiator)
 - Country B (conflict victim)
- Nature of company operations in each country (core business lines):
- Revenue exposure (%):
- Employee presence (local / expat):
- Key assets (physical, digital, IP):
- Current sanctions regime:
- Public posture to date (company statements, partnerships, etc.):
- Critical software and infrastructure in use:
- Third-party service providers (if any):
- Key stakeholders (shareholders, customers, governments, etc.):

Risk Mapping

Categorize risks and assess the likelihood and impact of each within the following categories. For each category, evaluate risks over the next [time horizon].

1. PHYSICAL RISKS

- Damage or disruption to physical infrastructure (e.g., facilities, warehouses)
- Identify secondary impacts (e.g., supply chain disruptions, currency fluctuations)

2. CYBER RISKS

- Identify threats to IT infrastructure, including network security, cloud services, and operational technology. Have any known cyber threat actors originating from [Country A] previously targeted [Country B]? If so, identify them by name and describe their past operations (e.g., DDoS attacks, spear-phishing campaigns, exploitation of zero-day vulnerabilities, etc.).
- Source code and dependency risks: Evaluate if the company's software dependencies (open-source, third-party) have known vulnerabilities or unpatched security gaps that could be exploited. Draw on open-source reporting from cybersecurity outlets (e.g., Bleeping Computer, CyberScoop) and major Western news organizations (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News).
- Risk of cyberattacks (e.g., ransomware, data breaches): Quantify the likelihood of disruptive cyberattacks and potential impact using threat assessments from cybersecurity firms (e.g., CrowdStrike, Mandiant), major technology companies (e.g., Microsoft), and official advisories from government agencies (e.g., U.S. CISA, the UK NCSC).

3. SOFTWARE SUPPLY CHAIN RISKS

- Audit the source code, third-party libraries, and open-source packages for known vulnerabilities or missing critical patches.
- Assess the risk of compromised or tampered dependencies in the development pipeline (e.g., via supply chain attacks).
- Evaluate the security posture of [Company's] software providers. Do any of them have a history of breaches or known vulnerabilities?
- Identify redundant systems or fallback mechanisms in case of service interruptions. Where do we lack redundancies in critical areas?

4. FINANCIAL RISKS

- The current sanctions picture is [fill in details]. Given past U.S. policies during this type of conflict, what type of sanctions do you anticipate will be forthcoming in the next six months of this conflict?
- Given that answer, assess the impact of those expected sanctions on revenue and operations.

5. LEGAL AND COMPLIANCE RISKS

- Identify areas where our company's operations could run afoul of sanctions regimes, including secondary sanctions from the U.S. or allied countries.
- Evaluate potential legal actions against the company (e.g., lawsuits related to alleged complicity in war crimes, genocide, or human rights abuses, and lawsuits related to breach of contract). Draw on DoJ indictments and official press releases, and UNHCR reports from previous, similar conflicts.
- Consider local laws that might change rapidly during conflict and could affect operations or employee safety (e.g., martial law, rule by decree, nationalized assets).

6. REPUTATIONAL RISKS

- Assess how the conflict is likely to affect the company's public image and brand perception. How might our actions in this conflict contravene our public statements and company values?
- Consider activism within the company, including employees or stakeholders publicly demanding action. Determine when employees have publicly protested company actions or issued open letters to management, and assess the outcomes of these activities. Draw on reporting from major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News).
- Identify potential media narratives that could emerge and damage public trust, such as accusations of unfair business practices, participation in unethical activity, corruption, or exploiting the conflict for profit.
- Assess whether the company is perceived as a neutral party, or if its operations could be seen as directly contributing to the conflict. Draw on official statements from both countries'

governments to assess whether (and how) they have publicly referenced the company since the outbreak of the conflict.

Recommendations for Immediate Action

Provide immediate actionable steps to address high-priority vulnerabilities, such as:

- Initiating vulnerability scans for source code and critical infrastructure
- Deploying emergency patch management for known threats
- Engaging with external security experts to address gaps in software dependencies
- Updating contingency plans to reflect the latest risk assessment

Decision Testing

Evaluate how these risks might change based on our decision to [stay in the conflict zone / partially wind down operations / segregate defense-related business / pull out of Country A / pull out of Country B / pull out of both countries]. Specifically:

- Does reputational risk worsen if we pull out of [Country B, or the “victim” country]?
- Does physical risk worsen if we only pull out of [Country A, or the “aggressor” country]?
- Do risks significantly improve if we segregate defense-related from civilian parts of the business? If we create a local subsidiary to manage defense-related business?

Risk Mitigation Strategies

Based on this risk evaluation, suggest mitigation strategies for these risks. Prioritize protection of company staff, including executive protection, diversification of critical supply networks, and narratives designed to ameliorate reputational risk.

PHYSICAL RISKS

- Employee evacuation plan (time frames, triggers, and external support from governments or NGOs). Has the company previously had to evacuate employees? If so, what did that plan entail, and how long did it take to execute? Draw on reporting from major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News) and official company statements.
- Location-based risk assessments for key infrastructure and staff. Are there specific regions within either country that present higher risk (e.g., proximity to military targets, densely populated urban areas, or strategic locations such as major ports servicing military vessels)? Draw on major Western news outlets (e.g., the *New York Times*, *Washington Post*, *Wall Street Journal*, and Fox News) and analysis from security-focused think tanks (e.g., ISW and CSIS) on each country’s military capabilities, force posture, and potential targets.
- Contingency plans for reducing company footprint in high-risk zones.

CYBER AND SOFTWARE RISKS

- Suggest a vulnerability management process for both internal code and external dependencies, with a focus on immediate patching and redundant systems.
- Suggest a schedule for accelerated audits of third-party dependencies and an implementation plan for dependency isolation to limit exposure to vulnerable or compromised packages.
- Construct a plan for implementing Zero Trust frameworks or network segmentation to reduce overall attack surface.

FINANCIAL RISKS

- Suggest several options for diversification of revenue streams in case the conflict leads to significant market or region loss.
- Suggest several alternative currency and asset options to protect against exchange rate fluctuations.
- Suggest talking points for discussion with legal counsel to anticipate potential penalties from sanctions. Suggest what questions we should ask our legal counsel.

LEGAL AND COMPLIANCE RISKS

- Develop an ongoing monitoring system to track changes in both international laws and local regulations.
- Suggest a schedule for us to regularly engage with compliance officers to ensure adherence to sanctions and humanitarian laws.

REPUTATIONAL RISKS

- Suggest a public communication strategy to clearly outline the company's stance in the conflict, balancing values with business continuity.
- Suggest standard operating procedures for spokespeople and legal teams to handle media inquiries and employee dissent regarding the company's position. Where could the company redirect backup resources and personnel to ensure this team remains adequately staffed?

Red Teaming and Stress Testing

ADVERSARY PERSPECTIVE

Use the results of the above analysis to stress-test the company's preferred risk mitigation strategy by adopting the perspective of external adversaries (e.g., cyberattacks, reputational backlash, legal penalties). [INSERT PREFERRED RISK MITIGATION STRATEGY HERE]

- Consider exploitative tactics used by adversaries (e.g., cyberattacks targeting critical infrastructure, phishing schemes aimed at employees) or public relations campaigns that could amplify negative sentiment.

- Propose adaptive strategies to counteract these potential attacks, with a focus on cyber defense and PR crisis management.

BOARD MEMBER PERSPECTIVE

You are now a board member of [Company] with expertise in physical and cyber security. Evaluate [Company Name]'s proposed course of action and contingency plan. Identify potential gaps in the proposal, with particular focus on security vulnerabilities to physical infrastructure protection and points of failure on our networks, as well as financial health and reputational effects. This should include assessments of both direct and cascading risks that could arise from unresolved issues in any of the categories.

Final Output

Provide a detailed risk evaluation report categorized by severity, likelihood, and strategic impact, alongside tailored mitigation and contingency recommendations to help the company make informed, timely decisions in this complex and evolving environment.

About the Authors

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president of the Defense and Security Department at the Center for Strategic and International Studies (CSIS). As the head of the INT Program, Harding provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. In her capacity as vice president of CSIS's Defense and Security Department, she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Harding has established herself as an expert on how technology is revolutionizing national security work. She has also served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At the Central Intelligence Agency, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House, her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the *Wall Street Journal*, BBC, NPR, Bloomberg, and other outlets. She holds a master's degree from Harvard University's Kennedy School of Government and a bachelor's degree from the University of Virginia.

Julia Dickson is a former associate fellow with the INT Program at CSIS. Her research interests included cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS,

she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Aosheng Pusztaszeri is a research associate with the INT Program at CSIS, where he focuses on emerging technologies and their implications for national security. Before joining CSIS, he interned in the U.S. Senate and the U.S. House of Representatives and served as an undergraduate research assistant in Cornell University's Department of Government. Aosheng holds a BA in government and history from Cornell University.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges. Founded in 1962, CSIS is led by General Joseph F. Dunford, who was appointed chief executive officer in 2026, succeeding John J. Hamre. The CSIS Board of Trustees is chaired by Thomas J. Pritzker, who has held the position since 2015.

CSIS brings together more than 275 full-time staff and a global network of affiliated scholars working across four core areas of public policy: defense and security, geopolitics and foreign policy, economic security and technology, and global development. Our scholars are regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer recommendations to improve U.S. strategy.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—non-partisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

What sets CSIS apart is not only the quality of its research but how that research is conveyed: through original data and open-source analysis; through multimedia and data visualization; and through connecting relevant analysis with key audiences at the moments that matter most. This combination of rigor, independence, and reach has made CSIS a driving force in the policy debates shaping American security and prosperity.

Endnotes

- 1 Arthur Herman, *Freedom's Forge: How American Business Produced Victory in World War II* (New York: Random House, 2012).
- 2 Eliot A. Cohen and Phillips O'Brien, *The Russia-Ukraine War: A Study in Analytic Failure* (Washington, DC: CSIS, September 2024), <https://www.csis.org/analysis/russia-ukraine-war-study-analytic-failure>.
- 3 National Council of Statewide Interoperability Coordinators, *Leveraging the PACE Plan into the Emergency Communications Ecosystem* (Arlington, VA: CISA, 2023), https://www.cisa.gov/sites/default/files/2024-10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.pdf.
- 4 "Google terminates 28 employees for protest of Israeli cloud contract," Reuters, April 18, 2024, <https://www.reuters.com/technology/google-terminates-28-employees-protest-israeli-cloud-contract-2024-04-18/>.
- 5 "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain," Chief Executive Leadership Institute, Yale School of Management, January 28, 2024, <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>.
- 6 Astha Rajvanshi and Yasmeen Serhan, "What to Know About the Global Boycott Movement Against Israel," *Time*, February 14, 2024, <https://time.com/6694986/israel-palestine-bds-boycott-s-starbucks-mcdonalds/>.
- 7 Patagonia Europe, "We are outraged. This war has no place in an equitable world—especially one in the grip of emergencies in energy and climate. The people of Ukraine need our help now," Facebook, March 11, 2022, <https://www.facebook.com/PatagoniaEurope/posts/we-are-outraged-this-war-has-no-place-in-an-equitable-world-especially-one-in-the/1286220698533428/>.

- 8 Anne Michel, “French NGO sues arms producer Eurolinks, seeking truth on alleged components delivery to Israel,” *Le Monde*, June 12, 2025, https://www.lemonde.fr/en/les-decodeurs/article/2025/06/12/french-ngo-sues-arms-producer-eurolinks-seeking-truth-on-alleged-components-delivery-to-israel_6742274_8.html.
- 9 Jonathan Stempel, “Unilever says it didn’t seek Ben & Jerry’s CEO ouster, urges lawsuit be dismissed,” Reuters, April 25, 2025, <https://www.reuters.com/sustainability/boards-policy-regulation/unilever-says-it-didnt-seek-ben-jerrys-ceo-ouster-urges-lawsuit-be-dismissed-2025-04-25/>.
- 10 Washington Post Live, “Brad Smith on Microsoft’s role in the war in Ukraine,” *Washington Post*, June 23, 2022, https://www.washingtonpost.com/video/washington-post-live/wplive/brad-smith-on-microsofts-role-in-the-war-in-ukraine/2022/06/23/de54fb87-d8ea-4fea-ab63-cc15c380aeac_video.html.
- 11 Brad Smith, “Defending Ukraine: early lessons from the cyber war,” Microsoft blog, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
- 12 Khrystyna Kvartsiana, *Ukraine’s Cyber Defense: Lessons in Resilience* (Washington, DC: German Marshall Fund, December 2023), <https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf>.
- 13 Brad Smith, “Microsoft suspends new sales in Russia,” Microsoft blog, March 4, 2022, <https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/>.
- 14 Ibid.
- 15 “Microsoft Stock Price Lookup,” Microsoft, <https://www.microsoft.com/en-us/investor/stock-lookup>; and “Microsoft Corporation (MSFT),” Yahoo! Finance, https://finance.yahoo.com/quote/MSFT/history/?guce_.
- 16 Dina Bass, “Microsoft slashes Russia operations after war clouds outlook,” Bloomberg, June 8, 2022, <https://www.bloomberg.com/news/articles/2022-06-08/microsoft-slashes-russia-operations-after-war-clouds-outlook>.
- 17 Ibid; and “Microsoft scales down Russia operations due to Ukraine crisis,” Reuters, June 8, 2022, <https://www.reuters.com/technology/microsoft-cuts-russia-operations-due-ukraine-invasion-bloomberg-2022-06-08/>.
- 18 Washington Post Live, “Brad Smith on Microsoft’s role in the war.”
- 19 Washington Post Live, “Brad Smith discusses online disinformation & how U.S. gov. & Big Tech can address it,” Washington Post Live, streamed live on June 23, 2022, YouTube video, 30:26, <https://www.youtube.com/watch?v=sWIBLuHybc0>.
- 20 Ibid.
- 21 Washington Post Live, “Brad Smith on Microsoft’s role in the war.”
- 22 Ibid.
- 23 Brett Iversen, Satya Nadella, and Amy Hood, “Microsoft Fiscal Year 2022 Fourth Quarter Earnings Conference Call,” Microsoft, July 26, 2022, <https://www.microsoft.com/en-us/investor/events/fy-2022/earnings-fy-2022-q4>; <https://www.cnn.com/2022/07/26/tech/microsoft-earnings>.
- 24 Mark Tyson, “Microsoft Disables Windows 10 and 11 Downloads in Russia,” Tom’s Hardware, June 21, 2022, <https://www.tomshardware.com/news/microsoft-disables-windows-10-and-11-downloads-in-russia>; and Lawrence Abrams, “Windows 10 and Windows 11 downloads blocked in Russia,” BleepingCom-

puter, June 20, 2022, <https://www.bleepingcomputer.com/news/microsoft/windows-10-and-windows-11-downloads-blocked-in-russia/>.

- 25 Ibid.
- 26 Daryna Antoniuk, “Russians will no longer be able to access Microsoft cloud services, business intelligence tools,” *The Record*, March 19, 2024, <https://therecord.media/russians-losing-access-microsoft-cloud-amazon>.
- 27 Ibid.; and Niva Yadav, “Microsoft suspends access to cloud services for Russian companies,” *Datacenter Dynamics*, March 20, 2024, <https://www.datacenterdynamics.com/en/news/microsoft-suspends-access-to-cloud-services-for-russian-companies/>.
- 28 Antoniuk, “Russians will no longer be able to access Microsoft.”
- 29 Bill Toulas, “Microsoft to shut down 50 cloud services for Russian businesses,” *BleepingComputer*, March 23, 2024, <https://www.bleepingcomputer.com/news/microsoft/microsoft-to-shut-down-50-cloud-services-for-russian-businesses/>; and Antoniuk, “Russians will no longer be able to access Microsoft.”
- 30 “Putin says services like Microsoft, Zoom should be ‘throttled’ in Russia,” *Reuters*, May 26, 2025, <https://www.reuters.com/technology/putin-says-services-like-microsoft-zoom-should-be-throttled-russia-2025-05-26/>.
- 31 “Microsoft unit in Russia to file for bankruptcy, database shows,” *Reuters*, May 30, 2025, <https://www.reuters.com/technology/microsoft-unit-russia-file-bankruptcy-database-shows-2025-05-30/>.
- 32 Anna Desmarais, “Iran Says It Will Attack 17 American Tech Companies in Middle East by April 1,” *Euronews*, March 12, 2026, updated April 6, 2026, <https://www.euronews.com/next/2026/04/01/enemy-technology-infrastructure-iran-threatens-amazon-google-and-microsoft-assets-in-middle>.



1616 Rhode Island Avenue NW, Washington, DC 20036
202.887.0200 | www.csis.org

FOLLOW CSIS

