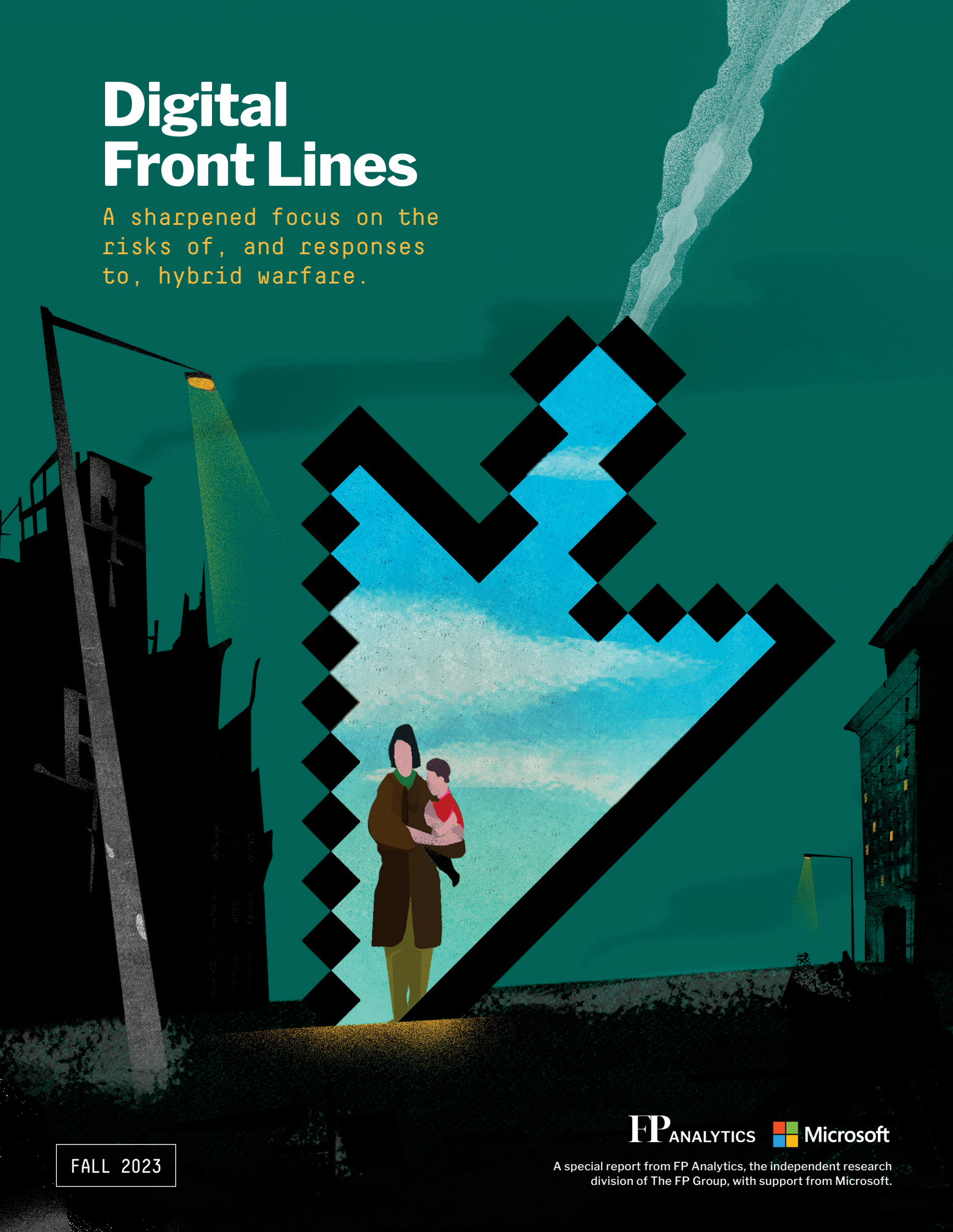
Digital Front Lines

A sharpened focus on the risks of, and responses to, hybrid warfare.



FALL 2023

FP ANALYTICS Microsoft

A special report from FP Analytics, the independent research division of The FP Group, with support from Microsoft.

An introduction from BRAD SMITH

Vice Chair and President of Microsoft

When I think about the war that has unfolded in Ukraine since February of 2022, three issues come to mind that underpin this partnership between Microsoft and FP Analytics and are grappled with in this project on hybrid warfare—Digital Front Lines.

The first is that, yet again, we are seeing technology change the nature of war. This has been an ever-present aspect of technological development that we saw accelerate in the 20th century. We first saw aircraft begin to enter the battlefield in World War I, and submarines posed new threats to Dreadnought warships during that same war. By World War II, the battleship's days were numbered as aircraft and aircraft carriers together changed the face of naval warfare. We saw the days of traditional trench warfare recede into the history books as well, as tanks proved that they could change how wars are fought on land. Now, in 2023, we're seeing a hybrid war in Ukraine that involves land, air, and sometimes sea, but frankly even more activity in cyberspace than on the water.

Part one of this report, beginning on page 4, considers how cyber operations are changing the nature of armed conflict.

However, there is also good news, which brings us to the second issue reflected in this report. Defenses in cyberspace have thus far won out on this new battlefield, defeating offensive cyberattacks because of defensive technology and the private and public sectors working together in Ukraine. This shows how important it is to continue to invest and innovate in the defensive protection of people online, both in times of peace, when cyberattacks have become all too common, and even more so during times of war. We've seen that advances in threat intelligence and the ability to dispatch code to defend digital devices through endpoint protection can make all the difference in contemporary warfare. And all of this is made possible because of a new dimension of public and private collaboration. Some of the important questions for the future are when, where, and how we sustain these partnerships. What are the proper roles for governments, tech companies, and NGOs alike?

As featured in **part two** of this report, beginning on page 20, a lot of lessons on these issues have emerged from the war in Ukraine, and it's important to capture, discuss, consider, and together define a path to the future.

This brings us to the third issue, and it's one I hope you all will continue to think about. We live in a world that needs strong international norms—norms around the conduct of war as well as how we protect the peace. This was such an important element to emerge from the 20th century, especially following the horrors and tragedies of World War II and the deaths of so many civilians. The world did the right thing by coming together in Switzerland in 1949 to adopt the fourth Geneva Convention, declaring that governments had not only a moral obligation but a legal duty to protect civilians in times of war. We need these kinds of norms to continue to stand firm and to adapt alongside the evolution of technology. This is a space where I believe so many of you can help contribute to not just the conversations but the decisive steps that will be needed in the years ahead.

> "This is the right time ... to take stock of how technology is changing the nature of war and to consider how it's calling for a new era and new forms of public-private collaboration."

Part three of this report, beginning on page 36, starts to explore these issues and what is needed to promote responsible behavior and improve cybersecurity in future armed conflicts.

This is the right time, in my view, to take stock of how technology is changing the nature of war and to consider how it's calling for a new era and new forms of public–private collaboration. It's time to think hard and act decisively to ensure that people around the world benefit from the international norms and protections they need and deserve online. ■

Illustration by KLAWE RZECZY

ABOUT THE PROJECT

The scale and scope of cyber operations in the lead-up to and since Russia's February 2022 full-scale invasion of Ukraine have been unparalleled and mark a new era of hybrid warfare in the digital age. The use of nonmilitary tactics—particularly cyber and information operations that leverage emerging technologies against military targets, civilian populations, and critical infrastructure to achieve foreign policy and geostrategic goals—present myriad pressing challenges for the prevention and resolution of conflicts. Recognizing the need to elevate awareness of cyber operations in armed conflict, FP Analytics produced Digital Front Lines with support from Microsoft.

In addition to deepening understanding of hybrid warfare, Digital Front Lines seeks to identify opportunities for collaboration across government, industry, and civil society to mitigate its destructive impacts. The contributions from experts in government, multilateral institutions, nongovernmental organizations, and the private sector along with research from FP Analytics underscore the need for sustained communication and coordination to adapt to the changing nature of warfare and effectively respond to the risks emerging from cyber operations.

PART ONE

Cyber Operations in Warfare—Ukraine and Beyond

FP ANALYTICS Microsoft

This special report was produced by FP Analytics, the independent research division of The FP Group, with support from Microsoft. FP Analytics retained control of this report, with overall direction provided by Allison Carlson (Executive Vice President) and Dr. Mayesha Alam (Vice President of Research) and research by Isabel Schmidt (Senior Policy and Research Analyst), Avery Parsons Grayson (Senior Policy and Risk Analyst), and Angeli Juani (Senior Policy and Quantitative Analyst). Edited by Diana D'Abruzzo. Art direction and design by Sara Stewart. Creative direction by Lori Kelley. Cover illustration by Brian Stauffer. Foreign Policy's editorial team was not involved in the creation of this content.

PART TWO

Multistakeholder Responses in Ukraine and Lessons Learned

Read the full report, with additional expert voices and interactive graphics, at

DigitalFrontLines.io

PART THREE

Preparing for Future Hybrid Wars

GLOSSARY

Belligerents: Persons, states, or groups engaged in war or conflict.

Civil–military coordination: Dialogue and interaction between military and civilian agencies, including in the government, private, and nongovernmental sectors, to facilitate efficient and effective processes.

Collective defense: The idea that an attack against one ally is considered an attack against all allies; the concept is enshrined in Article 5 of the North Atlantic Treaty, which formed NATO.

Content moderation: The process of detecting, removing, and otherwise responding to offensive or objectionable contributions on a platform.

Critical infrastructure: Assets, networks, and systems vital to the functioning of society, including for transportation, water, food, health, energy, information, and communication.

Cyber attribution: The process of identifying and disclosing responsibility for malicious cyber operations.

Cyber resilience: The ability to resist, withstand, and recover from malicious cyber activity.

Deepfake: An image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

Deterrence and defense: The strategy of preventing attacks coupled with limiting or mitigating the damage incurred by them.

Deterrence by denial: Persuading an adversary not to attack by convincing them that an attack will not achieve their intended goal.

Distributed denial-of-service (DDoS): A cyberattack that targets websites and servers by flooding a site with errant traffic, resulting in poor website functionality or knocking it offline altogether.

Dual-use technologies: Products that have a primary commercial application but also have the potential to be weaponized or used for military applications.

Foreign influence operations: Covert actions by foreign governments to influence another country's political sentiment or public discourse.

"Gray zone" tactics: The acts of state parties to a dispute maintaining high-level diplomatic relations while interacting antagonistically below the threshold of war.

Hack-and-leak operations: Incidents of data theft followed by the leaking of that information to the public.

Hybrid warfare: The use of nonmilitary tactics alongside conventional kinetic warfare to achieve foreign policy goals.

Information operations: Also known as influence operations, the collection and dissemination of information and propaganda about an adversary to advance strategic geopolitical goals.

International norms: Widely shared expectations about what constitutes appropriate behavior among governments and certain nonstate actors at the international level.

Kinetic warfare: Traditional military action that includes lethal force.

Multilateral institution: An organization of three or more states working together on issues of common interest, for example, the United Nations and NATO.

Multisector collaboration: Action and efforts across a range of international actors on a shared goal, such as cultivating and bolstering cyber resilience through technical, financial, diplomatic, and legal avenues.

Proxy warfare: A mode of war in which states with limited direct involvement in hostilities support or direct another state or party to the conflict.

Rome Statute: The treaty that created the International Criminal Court and defined the four most serious crimes under international law: genocide, crimes against humanity, war crimes, and the crime of aggression.

Rules of engagement: Directives that delineate when, where, how, and against whom military force may be used in a conflict.

Source code: The fundamental list of commands underlying a computer program.

Technical attribution: Using digital forensic tools to ascertain which software and hardware were used in a cyberattack.

Threat actor: Any organization, person, or group that directs an attack in cyberspace to cause harm against a specific target, including state and nonstate entities.

PART 1 | CYBER OPERATIONS

The Evolution of Cyber Operations in Armed Conflict

The digital domain is increasingly a battleground for state and nonstate actors who are leveraging capabilities in cyberspace to advance strategic geopolitical goals.

Hybrid warfare, the use of nonmilitary tactics alongside conventional kinetic warfare to achieve foreign policy goals, is hardly a new phenomenon. However, Russia's use of hybrid warfare techniques in Ukraine—particularly cyber operations—is unprecedented in scale and scope. Cyber operations, the use of digital technology to surveil, disrupt, corrupt, or destroy government, civilian, and information infrastructure, are a rapidly evolving and increasingly common method of attack, constituting a key domain of hybrid warfare. The frequency and variety of cyber operations in the ongoing Ukraine war have underscored the urgency of not only better understanding their manifestations but also identifying strategies to mitigate their destructive impacts.

This issue brief analyzes the evolution of cyber operations in contemporary armed conflicts. As part of the Digital Front Lines project, it brings sharpened focus to the compounding risks, emerging implications, and key opportunities related to the challenge of hybrid warfare.

Illustration by KLAWE RZECZY

Unpacking Cyber Operations in Armed Conflict

States have been selectively deploying cyber operations for more than a decade as part of their geopolitical strategy and to advance foreign policy goals—for example, when the United States and Israel reportedly deployed Stuxnet malware in 2010 to destroy 20 percent of Iranian nuclear centrifuges. One key reason that governments deploy cyber tactics is their plausible deniability—compared to conventional military action—which enables them to compel adversaries without triggering all-out war. Increasingly, however, including in Ukraine, cyber operations are being used as a prelude to, or alongside, military operations.

In Ukraine and elsewhere, threat actors are unleashing cyber operations to immobilize government services, sabotage critical infrastructure, disrupt elections, and achieve other objectives. In armed conflicts, threat actors are leveraging cyber tactics to augment kinetic operations. Moreover, threat actors are wielding cyber operations—such as those that generate and amplify disinformation—to weaken and undermine social cohesion, exacerbating political fragmentation.

In recent decades, cyber operations have played a central role in "gray zone" tactics, in which state parties to a dispute maintain high-level diplomatic relations while interacting antagonistically below the threshold of war. Nonstate threat actors may act independently or be affiliated with, and supported by, governments.

As cyber operations have become increasingly sophisticated and widespread, it is imperative for policymakers, business leaders, technical experts, civil society groups, and other stakeholders involved in addressing and mitigating cyberattacks to recognize and understand these tactics within the frame of hybrid warfare. Doing so is critical to avoid falling behind on the latest cyber developments and to foster collaboration to counter those threat actors who deliberately and indiscriminately harm civilians and civilian infrastructure for geopolitical advantage.

How Russia's Sustained Cyber Campaign Laid the Groundwork for Hybrid Warfare

While Russia's full-scale ground invasion began in February 2022, the Kremlin has been using cyber tactics to prime, destabilize, and coerce Ukraine since at least 2013, if not earlier. Russia has long waged a coordinated campaign of cyberattacks on government targets and information operations and has used cyber sabotage of critical infrastructure alongside its ground and air operations in Ukraine. Integrated cyber tactics used in Eastern Ukraine a decade ago foreshadowed Russia's hybrid approach to warfare in 2022.

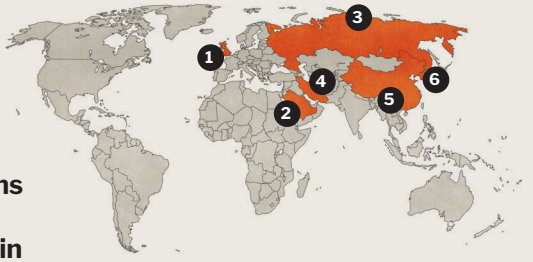
Spurred by the 2013 Maidan Revolution—a popular movement that shifted Ukraine into closer political alignment with the European Union and NATO—Russia began using cyberattacks to paralyze, discredit, and distract political opponents. Russia launched distributed denial-of-service attacks, for example, to offline the Maidan movement in 2013 and to take down government computer networks and communications in 2014, likely to distract from Russian troop presence in Crimea days before an internationally denounced referendum on annexation. Russian operatives also hacked Ukraine's electronic vote-counting

The Strategic and Tactical Utility of Cyber Operations

Priming
Interfering with and influencing targeted organizations to steer them into voluntarily making decisions that are harmful to their security, often using information operations. Also, gaining strategic access to civilian and government infrastructure, often in anticipation of tactical engagement.

Destabilizing
Conducting aggressive and visible attacks—including against critical infrastructure—with the aim of polarizing, demoralizing, and/or fragmenting the targeted organization and its constituents.

Coercing
Often combined with kinetic attacks, striking government and civilian infrastructure to compel a desired response from the targeted organization and its constituents.



Cyber Operations Are Not Solely a Russian Domain

As these examples illustrate, various threat actors use cyber operations for information warfare, high-publicity diplomatic statements, surveillance, and other goals.

1

U.K.

TARGET: ISLAMIC STATE

U.K. intelligence services attacked Islamic State communications technology in Iraq in 2018—disabling devices and providing false directives—to hinder the militant group's ability to coordinate and respond to kinetic attacks.

2

Saudi Arabia

TARGET: LIBYA

During the Libyan civil war (2014 onward), Saudi-backed companies allegedly deployed high volumes of bots before, during, and after key moments to prime local communities for attacks, exploit communal divisions, belittle resistance to the Libyan National Army, and discredit peace processes.

3

Russia

TARGET: U.S.

In 2019, Russian intelligence services allegedly injected code into a software update that infected at least 18,000 devices, including those at U.S. government agencies, allowing up to 14 months of deep and broad access to information before Microsoft, FireEye, and GoDaddy contained the malware with a kill switch in 2020.

4

Iran

TARGET: ISRAEL

In 2023, an Iran-linked group allegedly hacked, defaced, and disabled water controllers on at least 10 Israeli farms.

5

China

TARGET: TAIWAN

Before and during U.S. Speaker of the House Nancy Pelosi's visit to Taiwan in 2022, Chinese operators allegedly paralyzed Taiwanese government websites and projected anti-Pelosi and anti-Taiwan messaging on screens throughout the island.

6

North Korea

TARGET: WORLDWIDE

In 2017, "WannaCry" ransomware allegedly released by North Korea infected more than 200,000 computers globally, notably locking patient records on U.K. National Health Service computers, incapacitating the health service for several days.

system, delaying the results of the October 2014 parliamentary election.

In parallel, the Kremlin launched information campaigns on mainstream and social media aimed at priming local communities to support annexation. Russian-sponsored media, bots, and troll farms evoked and manipulated historical anxieties and divisions by connecting the pro-Western Maidan movement with a 20th-century Nazi collaborator and portraying Russia as the protector of all ethnic Russians and Russian speakers. International disinformation operations by Russia sought to deter and delay a response from the Ukrainian government and the international community by portraying Russian-backed separatists in Eastern Ukraine and Crimea as homegrown freedom fighters. These coordinated campaigns demonstrated Russia's capacity and willingness to deploy cyber tools to exploit and amplify societal divisions before, during, and after ground activity.

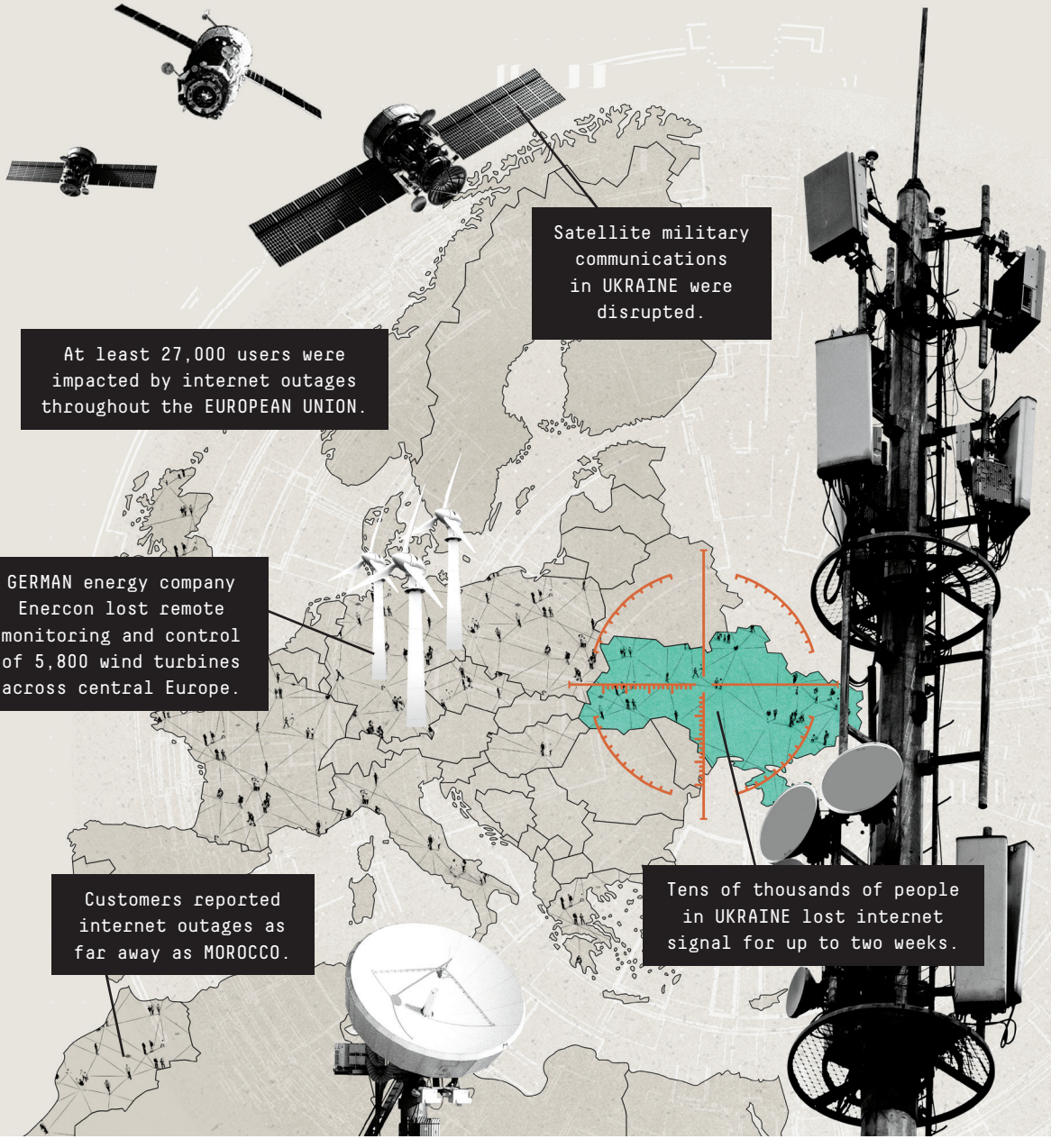
Even after Russia's ground operations in Eastern Ukraine and Crimea cooled in 2014, Russian cyber efforts to destabilize Ukraine and discredit the democratically elected government in Kyiv continued and were focused increasingly on sabotaging critical infrastructure.

In 2015 and 2016, Russian hackers targeted distribution substations near Kyiv, disrupting power supply to hundreds of thousands of residents for hours, impacting communications, emergency services, and other infrastructure. Russian malware targeted Ukraine's financial systems in 2017, causing around $10 billion in global damage. These far-reaching attacks, including the first-ever publicly acknowledged digital attack that caused a power outage, showcased the destabilizing potential for threat actors to exploit vulnerabilities in the online networks of critical infrastructure to inflict harm on, and incur costs from, civilians.

Disruptions Across Europe from Russian Satellite Hack

A cyberattack on the Viasat satellite network just hours before the Russian invasion of Ukraine had a cascading effect across the region.

On Feb. 24, 2022, one hour before the invasion of UKRAINE, Russia launched an attack using "AcidRain" wiper malware to remotely erase modems and routers on Viasat Inc.'s KA-SAT satellite network.



Data sources: CSO Online, Council of the European Union, CyberPeace Institute, La Depeche, Wired, Reuters, Zero Day

Cyber operations intensified in frequency and scale in the months leading up to Russia's full-scale invasion. From July 2020 to July 2021, Microsoft found that 19 percent of the global nation-state threat activity warnings they issued were made to customers in Ukraine, second only to the United States in that time period. On February 24, 2022, Russia launched its full-scale military invasion of Ukraine alongside a cyberattack on satellite modems that disrupted Ukrainian military communications. Since then, Russia has used coercive tactics—including DDoS, wipers, defacements, deepfakes, and scam emails—in an effort to discredit Ukrainian government targets, erode public trust, and demoralize Ukrainian society.

At times, cyberattacks have coincided with kinetic action, for example, when Russian military strikes and cyberattacks targeted government agencies in Dnipro simultaneously on March 11, 2022. However, the ways and extent to which Russia is consistently aligning its cyber and kinetic strategies are yet to be fully determined.

Cyber operations have concurrently targeted civilian critical infrastructure. According to Microsoft data, from February 2022 to October 2022, 55 percent of the Ukrainian targets hit by Russian wiper malware were critical infrastructure organizations, including energy, water, emergency services, and health care.

In April 2022, Ukraine thwarted a Russian attempt to take over electrical industrial control systems with the potential to knock out power to 2 million residents. All of this has occurred against the backdrop of an ongoing anti-Western, pro-Russian disinformation campaign within Ukraine and Russia, such as social media posts claiming that Ukraine was about to surrender unilaterally. In parallel, the Kremlin has worked to undermine international support for, and solidarity with, Ukraine, for example, by accusing Ukraine of using child soldiers and claiming that Russian-speakers in Eastern Ukraine have been subjected to genocide.

How Attribution Challenges of Cyberattacks Can Undermine Diplomatic Consensus and Decisive Response

As Russia's operations in Ukraine have shown, there are many challenges to attributing cyber operations accurately and verifiably. Some attacks—those for surveillance, for example—can go undetected or unreported for long periods of time, thereby complicating a timely identification and counteraction strategy.

Moreover, governments may choose to rely on proxies such as cyber mercenaries to deflect attention and maintain plausible deniability. They may also be constrained by intelligence-sharing protocols, while private organizations may be disincentivized from sharing perceived failures in their cyber defense capabilities. Barriers to making provable attributions and compiling evidence of attacks by public- and private-sector actors have the potential to undermine the swiftness and proportionality of diplomatic or military responses.

As international humanitarian law on conduct in armed conflict predates the proliferation of cyber operations, even when attacks are identified and attributed, a lack of agreed-upon and established international norms and legal frameworks to address cyber warfare poses a challenge. The *Tallinn Manual* represents a notable attempt by academics and practitioners to clarify concerns and codify approaches to cyberspace norms. Additionally,

Different Types of Cyberthreat Actors

A threat actor is any organization, person, or group that directs or facilitates an attack in cyberspace to cause harm against a specific target, including state and nonstate entities. Within the targeted organization, agents may be recruited by threat actors to serve as "insider" operatives who are motivated by profit or personal grievance and/or sympathetic to a political cause.

States
Operatives within a country's government, including, for example, military and intelligence agencies that direct cyber operations as part of the broader conduct of foreign policy.

Cybercriminals
Nonstate actors, both individuals and groups, who conduct cyber operations primarily motivated by profit.

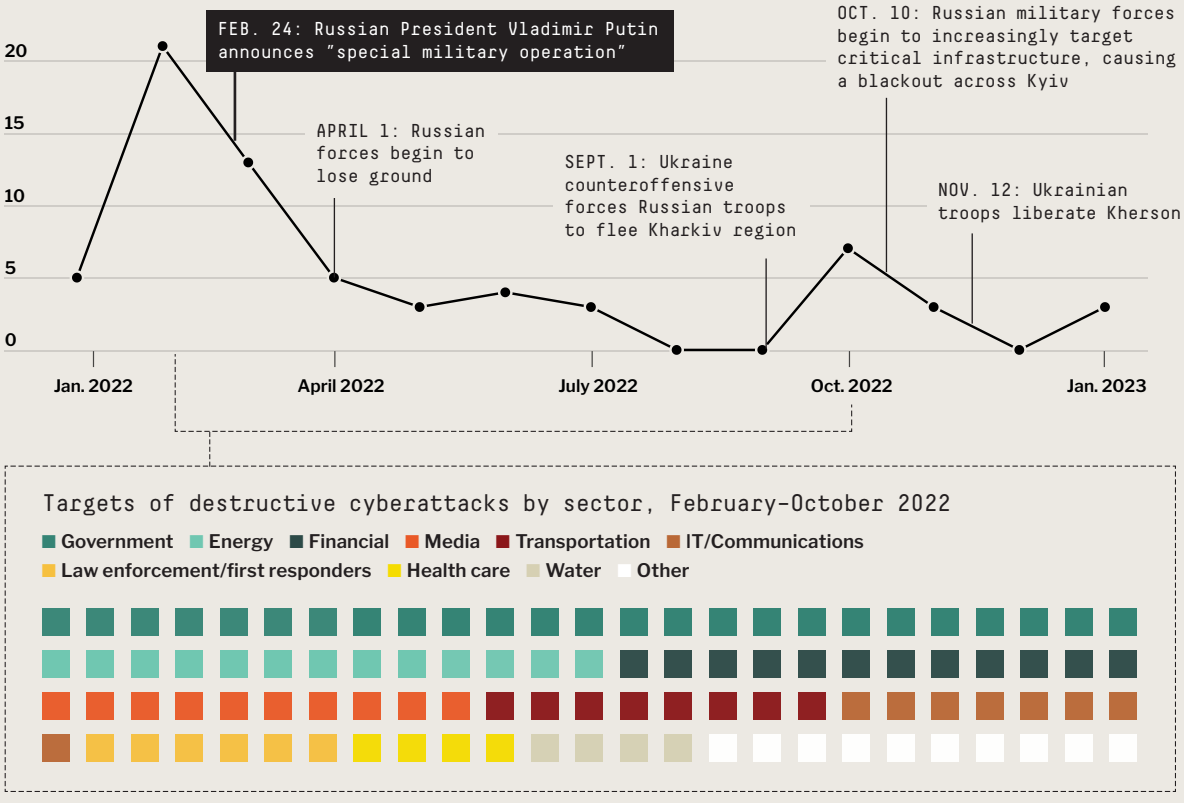
Hacktivists
Nonstate actors with a political motive, who limit their activism to the cyber domain. They may or may not be sympathetic to a particular state.

Terrorist groups
Nonstate actors who are ideologically motivated and often seek to sow discord or spread influence campaigns alongside physical attacks.

Cyber mercenaries
For-hire, private cyber operatives who are contracted by a state or nonstate actor for a specific operation or for the sale of specific technology.

Cyber Operations Ramped Up Preceding Russia's Full-Scale Invasion

The increase in number and scope of cyberattacks in Ukraine signaled a new phase of hybrid warfare.



Data sources: Microsoft, CNN

multistakeholder dialogues and working groups have been established at the regional, national, and supranational levels, including the United Nations' long-running Group of Governmental Experts and its more recently established (and Russian-supported) Open-ended Working Group, both of which seek to establish norms of behavior and the application of humanitarian law in cyberspace, and the U.N. Department of Economic and Social Affairs Internet Governance Forum (IGF). These initiatives provide the basis for greater international engagement and cross-sectoral collaboration to develop practicable approaches to mitigating and countering cyber operations and hybrid warfare.

Looking Ahead

Cyber operations have proven to be viable and effective weapons in the arsenal of state and nonstate actors worldwide. In addition to their strategic advantages—particularly ambiguity around attribution and proportionality of response—cyberattacks can be highly destabilizing and magnify the effects of kinetic warfare. As such, open, communicative, and collaborative relationships between the private and public sectors are crucial to anticipating, identifying, deterring, and responding to cyber operations, especially as social networks, hardware, and broadband internet serve as the vectors of many attacks.

The whole-of-society impacts of cyber operations call for a whole-of-society approach to deterrence. To that end, coordination across government, industry, and civil society stakeholders will be critical in Ukraine and beyond. Furthermore, developing global policies and guidelines on attribution, response, deterrence, and accountability on cyber operations will be critical to ending impunity, protecting national security, and creating international stability in the face of future hybrid warfare. ■

By Avery Parsons Grayson (Senior Policy and Research Analyst), Isabel Schmidt (Senior Policy and Research Analyst), and Dr. Mayesha Alam (Vice President of Research).

Cyber Resilience Helps Democracies Prevail Against Disinformation

The key is to mitigate attacks on communications systems and unmask attempts to corrupt infrastructure.

By ANNIE FIXLER

Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Before Russian troops poured into Ukraine in February 2022, the Kremlin had already begun its war online, using cyber operations to disrupt Ukrainian citizens' access to information and spread chaos and propaganda. This information warfare, however, has been met with the same resolve and resilience that Ukraine has shown on the battlefield, demonstrating for democracies around the world how to defeat authoritarian disinformation campaigns.

Information warfare often involves denying the adversary—domestic or foreign—access to information. During protests in Iran over the past four years, the regime has repeatedly throttled internet connectivity to try to prevent citizens who are organizing for greater freedoms from communicating with one another and the outside world. Russia has similarly tried—sometimes successfully—to use cyberattacks to disrupt Ukrainian military communications and citizens' access to information. But Kyiv had planned for such attacks—by, for example, ensuring that alternative systems were in place—and has been able to neutralize the assaults and restart service.

Authoritarian regimes also use cyber-enabled influence operations to contaminate the information environment, pushing false narratives and hiding their own human rights abuses. During the Beijing Olympics, for example, pro-Chinese Communist Party Twitter accounts flooded social media in an attempt to hijack hashtags created by dissidents who were trying to draw attention to abuses in Xinjiang. Throughout its war with Ukraine, the Kremlin has tried to muddy the flow of information to Ukrainians and distort global perceptions of the conflict. Russia has adjusted video evidence to deny war crimes, deployed operators on social media to create fake personas and news sites, and hacked user accounts to promulgate disinformation. Meanwhile, other Russian operations have tried to degrade confidence in the government in Kyiv. Hackers compromised a live Ukrainian news broadcast, inserting a false breaking news chyron claiming that Ukraine had surrendered. But Kyiv has been able to continue its YouTube broadcasts and social media posts to correct the record and reassure Ukrainians that their government still stands.

These attacks are meant to affect public behavior: Misinformation about fuel supplies during the May 2021 ransomware attack on the Colonial Pipeline caused panic-buying, leading to gas shortages. Russia has used radio broadcasts to urge Ukrainian soldiers to surrender. The Chinese Communist Party calls information operations "discourse power," reflecting an understanding that he who controls the conversation, shapes actions on the ground.

Countering Disinformation Requires Thwarting Digital Assaults

The Kremlin has failed to control the narrative in Ukraine because network defenders have kept communication infrastructure online, and the government in Kyiv has demonstrably shown Russia to be lying. Taiwanese civil society groups, meanwhile, are in a pitched battle to counter Chinese Communist Party disinformation about their leaders, among other fake news, because countering information operations requires not just keeping communication lines open but also thwarting the adversary's attempts to pollute them. Among the ways the Taiwanese have fought back are teaching schoolchildren about media literacy and creating news-verification tools.

This is what operational resilience against information warfare looks like: Mitigating attacks on communications systems so the adversary does not have an information monopoly, identifying the online infrastructure authoritarians use to promote false narratives, and unmasking attempts to corrupt the information environment. Future conflicts will see authoritarian states attempting to degrade access to information, control the narrative, and convince the public of the futility of the fight. But if the public can see that the enemy's attacks are failing because democratic countries have hardened their infrastructure and are quickly detecting the adversary's digital advances, not only will the enemy's cyberattacks fail, so will his disinformation campaigns. ■

Lessons from Ukraine in the Heat of an Ongoing Hybrid War

Ukraine has been building up its digital defense for the past decade—preparation that is now paying off.

By MYKHAILO FEDOROV

Vice Prime Minister for Innovations, Development of Education, Science, and Technologies and Minister of Digital Transformation of Ukraine

For the first time in history, a full-scale war between two countries has taken its fight online. The war in Ukraine is multidimensional: It's happening not only on an actual battlefield but also in cyberspace in the information arena. And we cannot underestimate either front.

On the day of Russia's full-scale invasion into Ukraine, February 24, 2022, I described our digital fight on the Telegram messaging app: "All night long we were defending cyberspace. Attacks on all basic information resources have been and are ongoing non-stop. Now everything is stable. All teams are on the ground. We remain calm and do not panic!"

To this day, we continue strengthening our digital resilience. What's the secret?

Because the fight against Russian attacks in cyberspace has been going on for more than nine years (you may remember the large-scale NotPetya cyberattack that struck Ukraine and then spread internationally in 2017), Ukraine understood the need to be resilient long before the full-scale war began in February 2022. Throughout 2021, we monitored various attacks on both the public and private sectors; that year, Ukraine ranked second in the number of cyberattacks against a specific country. Two weeks before the 2022 Russian invasion, we survived the largest distributed denial-of-service cyberattack in Ukraine's history. It was aimed at the banking sector and government websites—primarily those of the Ministry of Defense and Armed Forces and the Diia e-services portal, which provides Ukrainian citizens with access to online government services. But even that comprehensive attack could not break us.

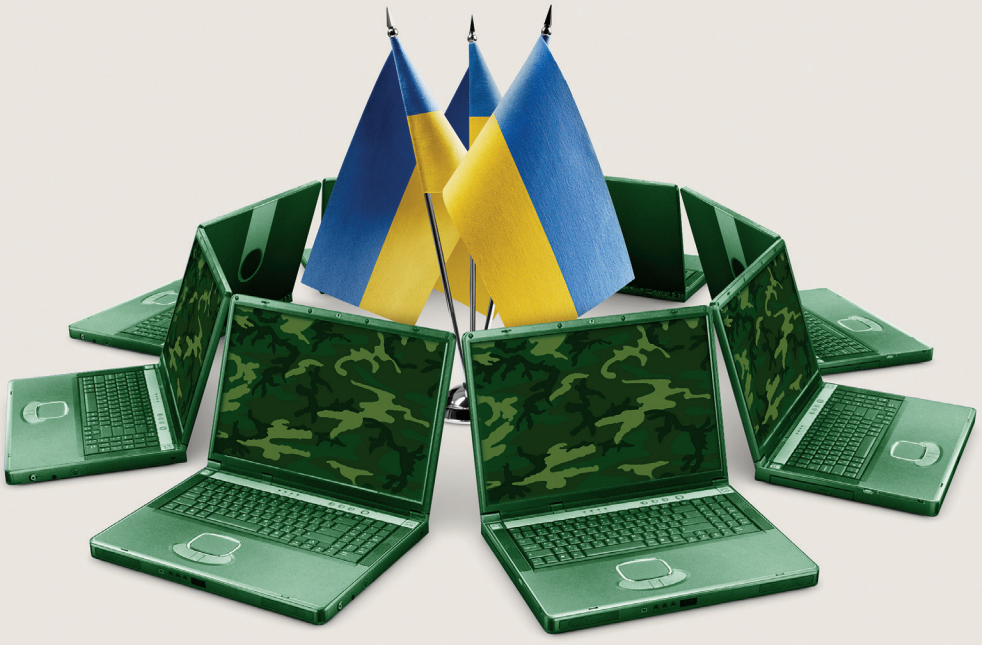
Cyberattacks intensified on the eve of the Russian invasion when the Russia-based threat actor Iridium deployed FoxBlade malware to destroy around 300 systems across more than a dozen government, IT, energy, agricultural, and financial-sector organizations in Ukraine. Jointly with Microsoft's Threat Intelligence Center, which had detected the launch against 19 government and critical infrastructure entities across Ukraine on February 23, 2022, we successfully reacted to the threats, and very little actual damage was sustained.

Overall, in 2022, more than 7,000 cyberattacks were detected in Ukraine, most of which were likely carried out by Russia. They were accompanied by increasing disinformation campaigns and coordinated with missile assaults. Such attacks are designed to commit espionage, spread lies through propagandistic operations—primarily to discredit the authorities—and destroy critical information infrastructure.

One vivid example: On April 1, 2022, an attack was carried out on Ukraine's governmental hotline center, which had been created to assist civilians during times of crisis and those affected by kinetic warfare. The attack involved injecting false data into the registry, aiming to falsely incriminate the Armed Forces of Ukraine for law violations in Bucha in March 2022. However, the reality was that Russian soldiers occupied the area and committed war crimes. This misinformation was then spread on social media to undermine international support for Ukraine. From January to March 2023, Ukraine registered far fewer cyber incidents: around 572, or two and a half times fewer than during the same period in 2022 when Russia's cyberwar against Ukraine heated up. Why? Both the government and Ukraine's businesses have significantly improved their cyber resilience; many institutions that disregarded the matter of cyber defense before the war have now made it a priority.

Strategies for Cyber Defense

Ukraine has managed to build an effective system of cyber defense at all levels, and it is based on three principles. The first is to deter cyberattacks with national incident management, response, and post-incident recovery systems. The second is to gain cyber resilience, which means strengthening national cyber preparedness for any possible attacks and creating a reliable



cyber defense system. The third is to improve the interaction and strengthen the coordination system among all authorities responsible for the state's cybersecurity and Ukraine's allies to share information and collectively build global resilience against cyber threats.

Before the full-scale invasion, one of Ukraine's fundamental solutions to cyber warfare was the creation of the Red Team of the Ministry of Digital Transformation, which crash-tests state information systems around the clock to find vulnerabilities. In December 2021, the Red Team's monitoring of the Ukrainian energy sector helped to improve the protection of information systems, and in the end, the energy sector withstood all hacker attacks with no damage.

In addition to the Red Team, the Ukrainian volunteer IT army has been essential; since February 2022, thousands of people from around the world have been helping Ukraine defend its digital borders. The Ukrainian government does not communicate directly with these IT soldiers, but in the beginning, the ministry helped with its coordination; anyone can join a Telegram channel to volunteer.

Another crucial key to Ukraine's success is cooperation. In order to secure the state, there must be permanent, systematic cooperation among the government and private and public companies. Transferring data registers to the cloud was one of the solutions that made it possible to work even when governmental agencies were attacked. By now, more than 100 state and critical information registers have been transferred due to cloud solutions and agreements with our foreign partners (among them, Microsoft Azure, Google, Amazon Web Services, Oracle, and the government of Poland). For instance, Amazon Web Services provides access to 10 million gigabytes of its cloud storage to back up Ukrainian government workloads to ensure the continuity of critical services.

As Ukraine has weathered blackouts caused by Russia's continued attacks on its infrastructure, cloud solutions and alternative communication methods—such as the Starlink internet satellite—have been critical to operating in the darkest of times. Literally.

Prevention Is Key

Governments and businesses can and should learn from Ukraine's experience fighting on the digital front lines. The prevailing lesson is this: It is easier to work to prevent attacks than to suffer their consequences. Just as governments rely on air defense systems to repel missiles, they should invest in creating cybersecurity iron domes to repel cyberattacks. They should hunt for and train the best cyber specialists. They should be constantly improving their cybersecurity and pursuing the most innovative solutions. And they should constantly be keeping their cybersecurity systems a few steps ahead. As attacks grow in complexity, it won't be long before artificial intelligence is used in this arena. The question is: Who will get there first—the governments or their attackers?

Governments and businesses that don't make cybersecurity a number-one priority won't survive. If it isn't a priority now, what are they waiting for? ■

Illustration by MATT CHASE

The Face of Modern Hybrid Warfare

Russia has aligned its cyber, military, and information operations in an unprecedented campaign.

By TOM BURT

Corporate Vice President of Customer Security and Trust at Microsoft

Russia's use of cyberattacks and cyber-enabled influence operations during its invasion of Ukraine has been a notable development in modern warfare. The scale of destructive and espionage cyberattacks and the sophistication of the global influence operations are unprecedented. And these cyber-enabled efforts have been coordinated with ground attacks in a manner that demonstrates how military strategy has transformed and likely will continue to evolve in the future. Since the beginning of the war, Microsoft has observed a Russian cyber and influence threat apparatus focused on undermining Ukraine's infrastructure and sources of support and degrading its will and ability to fight.

Cyberthreat actors associated with Russia's security agencies were involved in more than 600 instances of observed threat activity against more than 100 government and private-sector Ukrainian organizations in the first year of the conflict. Fortunately, this onslaught has largely been met with firm and effective resilience from Ukraine's government and its people, as well as the support of international partners across sectors. These events should nevertheless serve as a wake-up call to an international community that will need to grapple with the use of cyber operations in future hybrid conflicts.

Cyber-Military Alignment in Russia's Invasion

Alignment between Russia's cyber operations and its military operations on the ground has been evident from the earliest days of the war. Russian tanks started rolling across Ukraine's borders on February 24, 2022, but Microsoft security teams recognized that strategic Russian cyberattacks against Ukrainian targets had launched the day before. These offensive and destructive cyberattacks were intended to damage Ukraine's digital infrastructure in the hours before the full-scale invasion. This tactic of leading with cyber operations as the proverbial "tip of the spear" ahead of kinetic military operations—aiming to degrade infrastructure, disrupt supply lines, and/or mislead the public—is now a well-established practice in Russian military planning, dating to its 2008 war with Georgia.

Not only has digital technology been weaponized in this conflict, but digital infrastructure itself quickly became a prominent target. At the outset of the war, Russia successfully attacked Ukrainian satellite internet capability provided by Viasat. And some of the first Russian missiles targeted a government data center. The importance of uninterrupted access to information systems for government functions and national security made the physical locations of government data vulnerable targets. Simultaneously, destructive cyberattacks targeted key government

Wiper malware
Malicious software designed to permanently destroy data on an infected computer system.

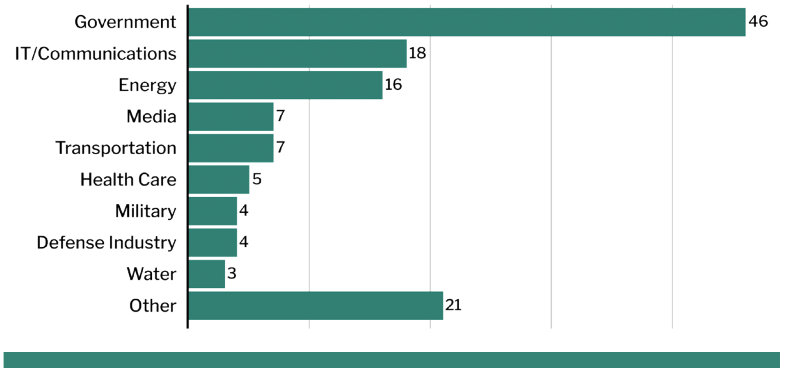
Ransomware
Malicious software that locks victims out of their systems by encrypting their data. Access is promised to be restored once a ransom is paid.

Phishing
Fraudulent digital communications meant to deceive victims into unintentionally providing attackers with privileged access or information.

> "Cyberthreat actors associated with Russia's security agencies were involved in more than **600 instances of observed threat activity** against more than 100 government and private-sector Ukrainian organizations in the first year of the conflict."

Partial List of Ukraine Targets

This chart provides a sample of Ukrainian sectors affected by known or suspected Russian state-affiliated network intrusions or destructive attacks, as reflected in Microsoft data between February 2022 and January 2023.



Data source: Microsoft Threat Intelligence 2023

operations and IT providers. Fortunately, Ukraine was able to move quickly to neutralize these threats by leveraging cloud computing to disburse and distribute government data across systems, both within and beyond its borders, creating redundancies that made attacks on any single data center ineffective.

Russia's military cyber operations in the war have been coordinated by threat actors affiliated with different government agencies, including military intelligence (GRU), the Federal Security Service, and the Foreign Intelligence Service. The use of wiper malware has been prevalent throughout the war. Microsoft has attributed these attacks to a GRU-affiliated threat actor group identified as Seashell Blizzard, otherwise known as Sandworm. To date, there have been at least nine separate variants of wiper malware used against targets in Ukraine, and in more recent months Microsoft has seen the development and use of new forms of ransomware as part of Russia's cyber arsenal. Meanwhile, other Russian threat actors, including Aqua Blizzard and Star Blizzard (aka Gamaredon and ColdRiver, respectively), have led espionage attacks seeking to compromise organizations—both within Ukraine and outside its borders—responsible for providing critical assistance and support to Ukraine. The chart above provides some insight into the sectors most targeted by Russia's cyberattacks in the first year of the war.

Coordination with Missile Attacks

Especially following the retreat of Russian forces from previously occupied territory in Ukraine last fall, there was a documented rise in Russian missile strikes targeting Ukrainian critical infrastructure like energy, water, and transportation systems. Last October, these attacks left 80 percent of Kyiv without running water and more than 10 million Ukrainians without power. Microsoft security teams observed coordinated destructive cyberattacks led by Seashell Blizzard targeting these same sectors. While we cannot know specific communications between the Russian military and its cyber operations, the common targeting and timing between the ground and cyber operations provide compelling evidence of a well-aligned war effort being executed simultaneously across multiple domains.

> For an interactive timeline of Russian military and cyberattacks on critical infrastructure in October 2022, visit **digitalfrontlines.io/the-face-of-modern-hybrid-warfare**

Influence Operations

Finally, influence operations online and in the media have also been a core component of Russia's invasion—both in Ukraine and in positioning Russia's objectives to audiences abroad. They have included flooding social media platforms with misleading messaging around the need for the "denazification" of Ukraine and accusing the United States of creating bioweapons in clandestine laboratories in Ukraine. Both of these narratives were intended to create a justification for the invasion. As the conflict has progressed, prominent news outlets backed by the Federal Security Service or other state-affiliated groups, such as NewsFront, have consistently supported anti-Ukrainian propaganda. Meanwhile, websites purporting to be Ukrainian local news have leveraged Russian state media sources to spread pro-Kremlin messaging that targets domestic audiences in occupied regions of Ukraine. Other influence operations have targeted European citizens in an effort to erode support for Ukraine's defense.

While the cyber tools and tactics employed by Russia in the invasion of Ukraine—destructive malware, espionage attacks, and information operations—are not themselves new or unique, the scale and coordination of their use as strategic components of a large-scale military campaign are truly unprecedented. And although Ukraine, working with partners, has successfully blunted much of the potential impact, we should assume that future conflicts will continue to deploy both cyber and influence weapons in novel ways. As with other military technologies, we should expect offensive capabilities in cyberspace to continue to evolve and become even more dangerous in the future. In response, governments and the international community need to work urgently to improve defenses, increase readiness, and make clear that illegal offensive actions in cyberspace will not be tolerated. ■

Tech Companies Are Fighting for Ukraine. But Will They Help Save Lives in Other Global Conflicts?

Much work is needed to determine how social networks and tech corporations can contribute to the broader efforts of preventing and resolving deadly conflicts.

By DR. COMFORT ERO

President and CEO of the International Crisis Group

Over the past few decades, nation-states have increasingly embraced the concept of hybrid warfare. Especially in situations short of open armed conflict, they are deploying cyberattacks, online influence operations, and other tech-enabled tactics to advance political goals and inflict harm on their adversaries. The war in Ukraine has led the United States and Europe to intensify their investment in hybrid warfare, but perhaps the most significant new developments have been the expanded roles played by Western technology companies and open-source researchers.

Over time, tech platforms have become important players in the international peace and security realm. With the war in Ukraine, a host of technology companies were on the front lines from the start and have turned into actors in hybrid warfare in their own right. Cyberattacks, a key feature of hybrid warfare, are aimed not only to cripple an adversary's defenses but also to probe and identify vulnerabilities in preparation for a larger attack. Russia had significantly more potent cyber warfare capacity than Ukraine, but tech companies helped Ukraine combat Russia's cyberattacks, transferred Ukrainian government data to remote servers to protect it from Russian airstrikes, and even provided free satellite internet coverage to soldiers and civilians behind enemy lines.

The immense public support for Ukraine after Russia's invasion also enabled the Ukrainian government to crowdsource its cyber response. When Moscow knocked Ukrainian satellite systems offline, open-source intelligence researchers from around the world provided information on Russian troop movements by using Google maps and images circulating online. Volunteers analyzed the immense data generated by the war to collect and provide information, including documenting potential war crimes. Ukrainian civil society and diaspora collected donations online to buy drones and off-road vehicles to support their soldiers and lobbied financial companies to modify their policies to allow such transactions.

The involvement of global digital networks and tech companies in Ukraine is far greater than it was in the Syrian civil war—sometimes referred to as the first social media war—and in many other relatively recent conflicts, including those in Libya, Yemen, Ethiopia, and Myanmar. In the case of Syria, social media platforms grappled with thorny questions of content moderation but neither resolutely confronted disinformation campaigns nor protected opposition and civil society accounts.

"When Moscow knocked Ukrainian satellite systems offline, open-source intelligence researchers from around the world **provided information on Russian troop movements** by using Google maps and images circulating online."

They did not archive digital records of war crimes in Syria, enabling users to delete incriminating evidence; courts later found that copies were inadmissible, because they could have been doctored. By contrast, the Ukrainian government persuaded Meta, Twitter, and TikTok to archive content to make it available to prosecutors pursuing war crimes cases in domestic, international, and foreign courts, which could help in holding perpetrators accountable.

Tech company participation in conflict- and atrocity-prevention activities around the world has been something of a hodgepodge. Some platforms, such as Twitter, Telegram, and Ushahidi in Kenya, have become hubs for crowdsourcing early warning information. Other startups and "tech for good" companies have answered government challenges to develop applications for everything from atrocity documentation to communications among conflict-affected communities. Yet, when it comes to tech's involvement in a major conflict, nothing comes anywhere close to the resources that private companies have mobilized on behalf of Ukraine.

What now? After robustly demonstrating some of their capacities to bolster the target of an unprovoked attack, tech companies may have raised expectations that they will continue to do so in the future. In a perfect world, these lessons would be exported to other conflicts. There is much appeal in the idea that private-sector actors might help civilians flee violence—guiding them to reliable information about access to medical aid, food, and safe shelter—and document the abuses they have experienced. Yet, it is hard to imagine tech companies taking the same bold actions in fights that are far from Western consciousness—particularly when public opinion doesn't line up clearly on one side, or U.S. government policy doesn't align with corporate preferences. There may even be cases where their engagement could be counterproductive or dangerous.

The war in Ukraine has shown how tech companies and social networks can be significant peace and security actors, but there is still much work to do. The international community must figure out how these companies can responsibly and reliably contribute to broader efforts to prevent, mitigate, and resolve deadly conflicts around the world. ■

Illustration by KLAWE RZECZY

Cyber Attribution Is Critical to Ensuring Accountability

As cyberattacks become increasingly common, calling out perpetrators is fundamental to imposing sanctions and taking countermeasures.

By CHRIS INGLIS

Former U.S. National Cyber Director

The anonymity that cyberspace provides is an all-too-valuable asset for malicious cyber actors, none more so than nation-states, which can fully exploit the cover of cyber operations for plausible deniability while still achieving strategic objectives. Peeling back the cover of anonymity and "lifting the veil" to identify the culprits of cyberattacks is critical to aligning actions with consequences and diminishing unacceptable behavior globally.

Given the complex weave of a globally interconnected system, cyber attribution—or the process of identifying and disclosing responsibility for malicious cyber operations—typically involves piecing together sometimes ephemeral digital clues, analyzing patterns of behavior, and finding similarities in tactics, techniques, and procedures with those of known threat actors. For nation-states, this process goes beyond a single-threaded technical exercise and involves significant use of both classified and unclassified intelligence sources to not only identify the threat actors perpetrating the attack but also the government, organization, or company that may be supporting or directing the operation. Take the deluge of cyberattacks that Russia has launched against Ukraine over the past year: U.S. and U.K. leaders have been especially quick to respond, and, after analyzing the evidence, publicly assign blame to the cyber actors—and the Kremlin that directed them—in an effort to mobilize those affected and minimize the harm caused.

Cyber attribution is a particularly critical element of an effective government response to cyber threats. It sets the stage and provides a public, political rationale for using instruments of power—be they diplomatic, financial, or otherwise—to curb and deter bad behavior. It is because of these consequences that states undertake a very formal and rigorous process of intelligence gathering and analysis before any determination is made. Though the process is often criticized for being lengthy and late and many times validating what is already assumed, the potential for state conflict requires a level of confidence and surety that only a rigorous process can provide. The diligence and discipline also act as a natural check against false flags and hasty assignments of blame—a worthwhile tradeoff given the potential implications of getting it wrong.

But cyber warfare's relevance in real-world crises increasingly requires surety *and* speed. The difficulty of achieving both at once has necessarily led to greater collaboration among defenders. No single nation-state or private company has the full picture of cyberspace threats, and it is only through collaboration and the pooling of resources that a critical mass of data points and evidence can be achieved quickly and with sufficient surety to underwrite the public actions that may result.

Intelligence-sharing partnerships, such as those among NATO countries and the Five Eyes, are critical to confirming the identity of an actor and bolstering the rigorous attribution process that each state undertakes. Indeed, cyber defense in foreign policy can be increasingly

> "Collaboration is by no means limited solely to states. The role of **the private sector in cybersecurity is central as the predominant provider of cyber infrastructure** and as 'first responder' to most incidents, including many that ultimately trigger state action."

characterized as a collective endeavor. Largely in response to cyber operations by China, Russia, North Korea, and Iran, the United States and its allies have increasingly used collaborative attribution to hold these states accountable and as a basis for diplomatic negotiation, economic sanctions, or the deployment of countermeasures. In 2020, the European Union took the unprecedented step of sanctioning China, Russia, and North Korea for previous attacks. In 2018, the United States, the United Kingdom, Canada, Australia, New Zealand, and others collectively attributed the NotPetya ransomware attacks to the Russian military. This kind of unified approach showcases the collective resolve of the international community and sends a strong signal that malicious behavior in cyberspace will not go unnoticed or unpunished. Collective action shares and dilutes the retaliation risk and financial cost that any one of them would bear if they were to make such a declaration alone.

Collaboration is by no means limited solely to states. The role of the private sector in cybersecurity is central as the predominant provider of cyber infrastructure and as "first responder" to most incidents, including many that ultimately trigger state action. To that end, the private sector has played an increasingly vital role in cyber attribution. Technology providers and cybersecurity companies have direct access and a scale of visibility to link individual attacks together into a discrete campaign that can be analyzed and then attributed to a single culprit. They are often the first to discover a large-scale campaign—and the first to provide a means to identify the perpetrator. When unveiled, the findings can create political will among the targets and governments to take formal action, including retaliation. Among the first and most notable such findings came from the American cybersecurity company Mandiant, whose APT1 report in 2013 exposed a large-scale cyber campaign by China's military. The report brought to light an issue—Chinese intellectual property theft—that until then had largely been limited to classified or policy channels, and it also set the tone for the role that the then-nascent cybersecurity indutry can play in attribution. Security firms like Novetta, Symantec, Crowdstrike, and others followed suit, helping to steer and focus U.S. and allied attention to emerging threats.

Though the private sector's role in cyber attribution is essential, it can have real-world consequences when the line between it and governments blurs. Assignment of public blame by a private-sector entity can create implicit agency if governments shape their positions or act against a foreign government. Compounding this challenge are differing norms and perceptions among states on the relationship between government and industry. Put simply, the Chinese or Russian governments' own close relationship with—or control of—industry may cause them to misread a U.S. company's attribution as a proxy for U.S. action. In this context, it is imperative that we preserve and safeguard the private sector's role in ensuring the resilience of our infrastructure and contributing its insight to cyber threats and avoid making it an active combatant in the deployment of powers reserved to states.

The ongoing conflict in Ukraine has demonstrated that cyber warfare is, and will continue to be, a dimension to state competition and geopolitics, as will cyber attribution. Establishing the intent and identity of the actor matters as much to private companies—which need to tailor defense to the operation at hand—as to states, which may need to mobilize public policy. Though the international community has made progress, attribution must continue to evolve to be more open, collaborative, and fast, built on ever-strengthening networks of information sharing, and bolstered by credible, public evidence.

The complexities of technology and sophistication of malicious actors to conceal their activity will never trend downward, nor will the consequences of cyberattacks. The stakes will get higher as the attribution problem gets harder. Working together and drawing on our collective strengths across borders and between the public and private sectors is the only way to avoid missteps and set a more sustainable path in cyberspace. As the cybersecurity industry has evolved, emerging collaboration and coordination has been essential and will continue to be ever more so in avoiding incidents or misunderstandings in international affairs. ■

Illustration by MATT CHASE

PART 2 | MULTISTAKEHOLDER RESPONSES

Cross-Cutting Responses to Strengthen Ukraine's Digital Resilience

How various international stakeholders have worked together to mitigate cyberattacks in the ongoing hybrid war.

Despite an established pattern of cyber operations against Ukraine dating to at least 2013 and warnings of an impending "cyber-Armageddon," Russia's cyber offensive since the full-scale invasion in February 2022 has found limited success. While it is likely that some operations—for example, those in the priming stages, including surveillance—may have gone undetected or unreported, Ukraine's cyber resilience has, with international support, largely prevailed in the face of sustained Russian cyberattacks against the government and population. This issue brief analyzes the international community's multisector collaboration to respond to Russian cyber operations and strengthen cyber capacity. Beyond insights on Ukraine, the successes and challenges examined here can inform preparation for future cyber–kinetic conflicts.

Illustration by KLAWE RZECZY

Ukraine has continually built up and adapted its cyber defense capacity since Russia annexed Crimea in 2014. As a result, the country has significantly deterred, defended against, and mitigated the cyber destruction that Russia and its proxies have unleashed since February 2022. Notably, international actors have helped to bolster Ukraine's cyber resilience through technical, financial, diplomatic, and legal avenues. International governments, along with private-sector companies, multilateral institutions, media outlets, and civil society stakeholders, have partnered with one another and Ukrainian actors to prevent and blunt the effects of cyberattacks. In particular, the private sector's level of involvement has been unprecedented; multinational companies have directed their technology and expertise to aid Ukraine, responding to Russian cyber operations by countering mis- and disinformation, including through public reporting on malicious activity, providing access to proprietary technology, building digital capacity, and assisting with cybersecurity strategies.

In-Kind Contributions Have Strengthened Ukraine's Cyber Resiliency

The international community has mobilized to protect Ukraine's ground and digital defenses in numerous ways, including offering subject-matter expertise and intelligence to protect critical infrastructure and government data. These efforts demonstrate models for cyber cooperation on a cross-sectoral and sub-government level. In the months before Russia's full-scale invasion of Ukraine, an EU-U.S. cyber response team was dispatched to Ukraine to detect active cyber threats and build defensive capacity.

As Russian Cyberattacks Ramped Up, Ukrainian Actors Accelerated Response Times

The Ukrainian responses to three similar attacks on the electrical grid since 2015 show significant improvements in cybersecurity protocols by critical infrastructure operators.

December 23, 2015

Attack: Russian military cyber unit Seashell Blizzard (aka Sandworm) targeted three energy providers near Kyiv, based on a May 2014 infiltration, remotely disconnecting approximately 30 power substations and inundating customer support centers with calls, while attempting to delete data from affected computers.

Impact: The resulting power outage affected 230,000 people in western Ukraine.

Response: Ukrainian responders neutralized the attack by switching to manual control within **360 minutes**.

December 17, 2016

Attack: Seashell Blizzard used a more advanced technique to once again target energy providers, attempting to trigger automated protective systems to take substations offline.

Impact: One power substation near Kyiv was successfully taken offline, disrupting 202.9 megawatts of power (the estimated daily usage of 600,000 Ukrainian households).

Response: Government-operated electricity company Ukrenergo promptly switched to manual control, restoring power within **75 minutes**.

April 8, 2022

Attack: An updated version of the 2016 malware, attributed to Seashell Blizzard, targeted several electrical substations in a two-pronged attack, as one program aimed to cut power while the other wiped data.

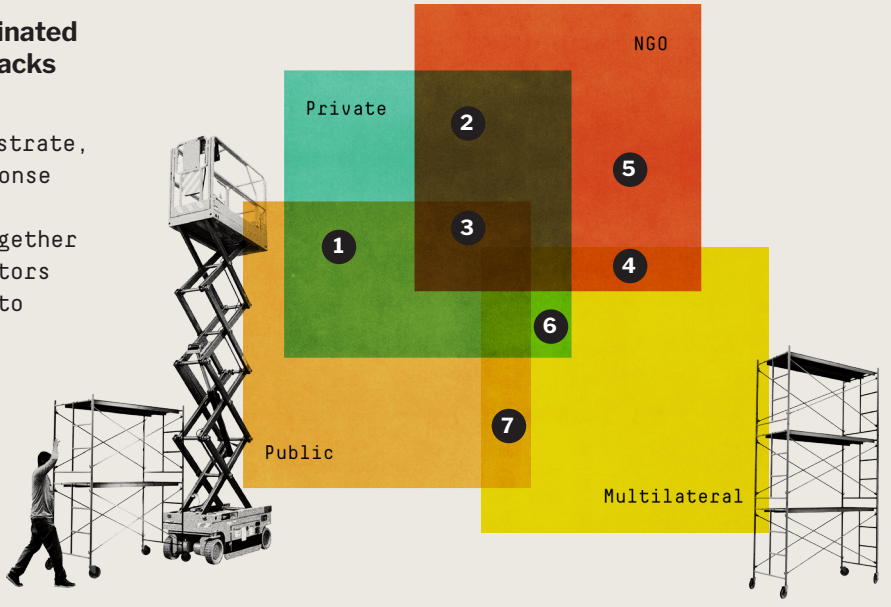
Impact: The attack, if successful, would have affected up to 2 million people.

Response: Ukrainian authorities reportedly thwarted the attack before it affected power supply or damaged the grid. **0 minutes**

Data sources: E-ISAC, International Security, Reuters, The New York Times

Multiple Sectors Coordinated Responses to Cyberattacks Targeting Ukraine

As these examples illustrate, the international response to cyber operations in Ukraine has brought together actors from across sectors to respond creatively to cyber threats.



1 Public-private

With support from USAID, SpaceX sent more than 5,000 Starlink satellite internet dishes to Ukraine days after Russia's full-scale invasion. Following controversy regarding continued funding and use-restrictions for Starlink, the U.S. Department of Defense purchased the satellite internet terminals to ensure continuity for Ukrainian defense.

2 Private-NGO

Microsoft partnered with Danish nongovernmental organization International Media Support to assist the Center for Strategic Communication and Information Security within Ukraine, creating a secure communications platform to improve information-sharing and response within and among the private sector, NGOs, and journalists in Ukraine.

3 Public-private-NGO

The U.S. Department of State launched the multimillion-dollar nongovernmental Conflict Observatory in May 2022 in partnership with Alcis and the Environmental Systems Research Institute to analyze, verify, and publicize Russian war crimes and atrocities committed during its invasion of Ukraine.

4 Multilateral-NGO

In March 2023, the Human Rights Center submitted its second Article 15 communication to the International Criminal Court (ICC), arguing that the ICC should investigate five Russian cyberattacks due to their targeting of civilian objects and their indiscriminate nature, and that the potential economic, political, and psychological harm to civilians satisfies the ICC's threshold of "gravity."

5 NGO

Since the invasion, the Geneva-based CyberPeace Institute has published quarterly analyses of cyberattacks in Ukraine, tracking harm to civilians and highlighting relevant legal instruments for addressing cybercrimes.

6 Multilateral-private

The G7's Rapid Response Mechanism, announced in 2018, dedicated funds and technical assistance to increasing the cybersecurity of newsrooms in Ukraine and neighboring countries that have been similarly subjected to Russian information operations, such as Moldova.

7 Multilateral-public

The U.N. Development Programme announced a competition in March 2022 for countering fake news, disinformation, and propaganda in Ukraine as part of a larger program to digitalize public services in Ukraine.

Data sources: Bloomberg, The Guardian, Microsoft, Spravdi Ukraine, Conflict Observatory, CyberPeace Institute, Government of Canada, Bellingcat, UC Berkley Human Rights Center, OpinioJuris, UNDP

Individual U.S. government agencies have also leveraged existing relationships and established partnerships to develop cybersecurity and connectivity in the Ukrainian private sector. The U.S. Department of Energy, for example, has worked closely with the energy sector in Ukraine to increase cyber defenses and alleviate damage; the U.S. Treasury has likewise supported the National Bank of Ukraine to improve cybersecurity and information-sharing across the financial services sector, guarding against such attacks as 2017's NotPetya. Additionally, the U.S. Agency for International Development (USAID) has provided emergency technological support—including more than 6,750 communications devices, such as satellite phones and data terminals—to government agencies, critical infrastructure operators, and emergency services to stanch the crippling effects of repeated cyberattacks on telecoms infrastructure.

Alongside digital capacity-building and in-kind contributions from allied governments, Ukraine's cyber defense has also benefited significantly from far-reaching private-sector technical assistance and proprietary services. The Ukrainian Ministry of Digital Transformation has maintained a close partnership with companies including Microsoft, Amazon Web Services, Google, Oracle, and Starlink. In particular, the rapid action taken to evacuate Ukrainian government data to remote servers and the cloud demonstrates the impact of public–private collaboration to safeguard data digitally and physically. Some tech companies have likewise supported the Ukrainian private sector at reduced or no cost. Microsoft has provided cloud-computing platforms to companies including Kernel, Ukraine's largest producer of sunflower oil, and KredoBank in order to bolster critical infrastructure resilience. In July 2022, Cloudflare offered free rapid cyber defense services to more than 60 Ukrainian businesses that were concerned they had been breached by Russian hackers. The expertise, capacity, and agility of the private sector have been critical to safeguarding Ukrainian cyberspace and public and private data.

International Financial Support Has Buttressed Ukraine's Cyber Defense

The direct funding that Ukraine has received, particularly from governments, has been invaluable in supporting Ukraine in custom-building its cybersecurity infrastructure to better defend against Russian operations. Public-sector and multilateral donations and financial support have included a focus on such critical infrastructure as telecoms, internet, and health services. These donations also included funding to connect Ukrainian government agencies to commercial cybersecurity companies and foster partnerships with tech companies to deliver the necessary resources and support.

Nongovernmental organizations have also taken steps to directly fund Ukraine's cyber response. For example, U.S.-based nonprofit UkraineNow.org originally focused on directing public donations to refugees but expanded its remit in August 2022 to include fortifying cybersecurity infrastructure. The global public can now donate directly to support the purchase of stronger login credentials for Ukrainian government agencies including the National Police, the Ministry of Digital Transformation, and government-owned energy and power plants. By contrast, while private-sector companies have donated significant sums to humanitarian and civil society organizations active in Ukraine, few, if any, have specifically directed funds toward cyber defense. Instead, with a few exceptions, contributions to Ukrainian cyber resilience have largely taken the form of in-kind donations of services and technologies.

Diplomatic Actions Have Targeted Russia's Cyber Capacity, While Bolstering Ukraine's

International support for Ukraine has taken various forms beyond financial and technical assistance. Many international actors have responded to Russian aggression in Ukraine by using their diplomatic clout to condemn Moscow and impose punitive measures. Furthermore, states including Australia, Japan, Norway, South Korea, the United States, and the United Kingdom have imposed restrictions to weaken Russia's technical capacity to launch cyber operations, limiting exports to Russia of dual-use tech products such as semiconductors, information security equipment, lasers, and sensors. Of note, some sanctions have targeted Russian organizations and individuals, including those to which cyberattacks were attributed prior to the war. The EU has regulated cyber activity, sanctioning Russia's tech sector, prohibiting IT consultancies from working in Russia, and prohibiting Russian nationals from holding executive positions in EU critical infrastructure. A range of multinational companies have likewise isolated Russia's cyber infrastructure in line with sanctions. Tech companies including Apple, ESET, and Microsoft significantly scaled down services from the Russian and Belarusian markets following the full-scale invasion. Engineering software companies including Autodesk, Dassault Systèmes, and PTC have done the same.

Diplomatic responses have not only isolated Russia but also have rallied around Ukraine. The North Atlantic

Rapid, Collaborative Efforts Supported the Safe Evacuation of Ukrainian Government Data to the Cloud

A timely private-public partnership moved critical government information and operations to the cloud just before the Russian invasion.

Pre-February 17, 2022

Up until one week before Russia's full-scale invasion, Ukrainian government operations were entirely located in on-premise servers. Ukraine's data protection laws—like those of many other countries—prohibited processing and storing government data in the public cloud.

February 17, 2022

Following Vice Prime Minister and Minister of Digital Transformation of Ukraine Mykhailo Fedorov's advocacy, Ukrainian parliament amended data protection laws to allow the evacuation of critical government data.

February 17, 2022–December 2022

A coalition of tech companies partnered with the Ukrainian government to move information and operations to the cloud. Microsoft committed $107 million in technology support, including cloud data storage solutions. Amazon Web Services was also pivotal to these efforts, physically transporting data servers into Ukraine and then back over the border once information had been transferred, before uploading data onto the AWS cloud.

February 24, 2022

These efforts were timely and impactful. On the first day of the invasion, Russian missiles targeted a Ukrainian government data center while Russian wiper cyberattacks also targeted government on-premises networks.

Early May 2022

Much of the Ukrainian government's essential digital operations and data were transferred to the cloud, including the work of 20 ministries and more than 100 state agencies and state-owned enterprises.

By the end of 2022

An estimated 10 million gigabytes of Ukrainian government data were being stored on cloud-based platforms. According to Minister Fedorov, more than 100 state databases have been transferred to servers across Europe, and onto cloud platforms, although Ukraine has been careful not to disclose where servers are located.

Data sources: Microsoft, The Stack, Foreign Policy, Insider, TechRadar

Illustration by KLAWE RZECZY

Treaty Organization (NATO) responded to cyberattacks in Ukraine by strengthening diplomatic ties with Kyiv and committing to increased investment in regional cybersecurity. Days after Russia's invasion, NATO upped its diplomatic deterrence by reiterating that a cyberattack could trigger collective defense through Article 5. Furthermore, NATO admitted Ukraine to its Cooperative Cyber Defence Centre of Excellence—which conducts training and research and hosts the world's largest international cyber defense exercises—in January 2023 as a "Contributing Participant." This invitation demonstrated a creative solution for supporting Ukraine while avoiding the governance challenges associated with adding new members to the alliance. Still, many multilateral institutions have been constrained by institutional challenges, such as the inability to use existing conventions in situations below the threshold of war, and Russia's veto power in the U.N. Security Council.

Prosecution of 'Cyber War Crimes' Could Set Precedent for Future Conflicts

International actors have also been engaged in a dynamic legal effort to hold Russia accountable for its cyber actions and establish norms for future cyberattacks. In 2021, NATO's Cooperative Cyber Defence Centre of Excellence launched the *Tallinn Manual* project, the world's most comprehensive effort to codify international norms regulating cyber behavior and identify important areas of nonconsensus for further investigation. The UC Berkeley Human Rights Center partnered with the U.N. Human Rights Office to launch the Berkeley Protocol in January 2022 to guide the verification, collection, and analysis of open-source intelligence for use in international investigations, including distributed denial-of-service attacks, phishing attacks, malware, and other cyberattacks.

Leveraging international law, the Human Rights Center formally requested in May 2022 that the International Criminal Court (ICC) indict a Russian-backed group for the targeting of civilian utilities in Ukraine, urging the prosecutor to include cyberattacks in his investigations. In March 2023, the center submitted its second request to the ICC, arguing that the ICC should investigate five Russian cyberattacks due to their indiscriminate nature and targeting of civilian objects. While there is currently no consensus on whether cyberattacks qualify as war crimes under existing statutes, if taken forward, these complaints would be the first instances of the ICC investigating cybercrimes and could lead to new efforts to adapt international humanitarian law to digital warfare.

Preparing for the Next Hybrid War

Aided by a rare Western consensus on Russian aggression, the ongoing war in Ukraine has led to novel multisector collaboration to deter and respond to cyber operations and build long-term defenses. Exceptional levels of private-sector involvement have significantly enhanced cybersecurity but have also elevated new challenges. Norms around responses to cyber operations are in the process of being established, but the lack of clear guidelines creates difficulties for all actors, including how to work collaboratively across sectors. For instance, mutually agreed expectations have not yet been established for public-private partnership in cyber warfare, and potentially divergent aims and motivations could create a disconnect between public and private interests.

$83M

Since 2016, the United States has donated more than $83 million to strengthen Ukraine's cybersecurity capacity and protect essential networks and infrastructure (2016–June 2023).

$8.5M

The United Kingdom donated $8.5 million to support Ukrainian government cyber infrastructure, including funding to connect Ukrainian government agencies to private-sector cybersecurity expertise (February 2022).

$4.7M

The European Bank for Reconstruction and Development donated $4.7 million to enable Ukrainian internet connectivity to bypass the national grid (December 2022).

$430M

Microsoft donated $430 million in cash and services to all sectors in Ukraine (as of February 2023).

$45M

Google.org donated $45 million in cash and services to all sectors in Ukraine (as of February 2023).

$35.1M

The EU announced the investment of $35.1 million over three years to support Ukrainian military, medical, and cyber defenses (February 2022).

The private sector's close involvement in the formulation and implementation of cyber defense policy can simultaneously create opportunities and raise ethical challenges. While there are normative reasons for companies to act against Russian cyberattacks, private entities can also benefit from high-profile international responses through reputational boosts and product exposure. Furthermore, operational difficulties may arise if companies' profit motives or shareholder responsibilities prevent them from offering technology and expertise indefinitely. If the beneficiaries of in-kind aid do not adapt rapidly, or if other partners do not step in to assist, an unplanned or rapid withdrawal has the potential to leave cyber defenses exposed. Governments stand to benefit from strategic planning to sustainably maintain long-term cyber capacity and support, including creating mutually agreed expectations for private-sector involvement without over-relying on companies for services and technology.

The collective response to the Russian invasion has showcased new strategies to prepare for, and respond to, future wars in which cyber operations could play an even greater role; as such, there is much to learn from the ongoing innovation and collaboration taking place in Ukraine. The input and support of international partners demonstrate the potential impact of a whole-of-society, consensus-driven approach to defense against information warfare and cyberattacks. Cross-agency intelligence-sharing and technical assistance can effectively build upon existing intergovernmental relationships and create new alliances. Critically, the private sector can provide vital expertise, creativity, and manpower in providing cyber defense services and capabilities. Furthermore, the Russia–Ukraine war—and the preceding decade of cyber operations—underscore the need for long-term cyber strategies to manage the emergence and escalation of potential future instances of cyber–kinetic conflict in geopolitical hotspots such as China, Iran, or North Korea.

The lessons learned from Ukraine's cyber resilience and the cooperative multisectoral support of the international community can be drawn upon to prepare for future cyber threats around the world:

- In December 2022, the European Bank for Reconstruction and Development partnered with a Ukrainian global cybersecurity service provider (ISSP) to share best practices and lessons learned to enhance the cybersecurity of businesses in Moldova—a country that has experienced a dramatic rise in cyberattacks since Russia's invasion of Ukraine.
- Estonia is working with Ukrainian partners to adapt and implement Ukraine's resilient online platform for public services and data storage.
- In the Dominican Republic, the Latin America and Caribbean Cyber Competence Centre is elevating lessons learned from Europe, including Ukraine, to assist regional governments in developing cyber strategy and capacity.
- NATO's 2022 Strategic Concept, which defines the security challenges facing the alliance and outlines the efforts needed to address them, includes such tasks as enhancing cyber defenses, networks, and infrastructure; increasing investment in emerging technology and cooperation with the private sector; and developing standards to protect democratic values and human rights in cyberspace.

While these initiatives are promising, there is much to be done, not only to further support and strengthen cyber defenses but also to improve communication, coordination, and collaboration globally in the age of hybrid warfare. ■

By Isabel Schmidt (Senior Policy and Research Analyst), Avery Parsons Grayson (Senior Policy and Research Analyst), and Dr. Mayesha Alam (Vice President of Research).

Diverse Public and Private Initiatives Countering Mis- and Disinformation

The proliferation of digital mis- and disinformation—including through foreign influence operations—in Ukraine and beyond has led to novel containment and media resilience strategies. Initiatives such as the nongovernmental Center for International Media Assistance program and the G7's Rapid Response Mechanism have helped to secure Ukrainian newsrooms in spite of repeated kinetic attacks and cyber operations. Multilateral institutions such as the EU and NATO have established task forces to counter disinformation and bolster media trust, while independent NGOs such as UkraineFacts and Vox Ukraine have provided fact-checking. Alongside the EU's suspension of licenses for several Russian-backed media outlets, private companies have taken action: YouTube, for example, removed at least 85,000 videos and 9,000 channels by February 2023 for spreading Russian propaganda.

Governments and private entities have also countered mis- and disinformation through direct information-sharing. The Government Information Cell has worked with allies to coordinate messaging and share intelligence. U.S. agencies have held regular public briefings and intelligence-sharing protocols with the Ukrainian government—an unparalleled arrangement with a non-NATO member. Additionally, companies such as Google and Microsoft have regularly shared threat intelligence on cyberattacks. These and other initiatives supported efforts to counter misinformation regarding Russia's cyber campaign.

Strategies for Reconciling International Humanitarian Law and Cyber Operations

A Q&A with
DR. PETER MAURER

President of the Basel Institute on Governance and former President of the International Committee of the Red Cross

As the world adapts to hybrid warfare, cyber operations like data breaches are having an impact on the ability of humanitarian organizations to protect civilians, thereby increasing the potential human costs of conflict. Cyberattacks on critical infrastructure such as energy grids, telecommunications networks, or digital hospital systems can also undermine the well-being of civilians in a variety of ways. While some organizations such as the International Committee of the Red Cross (ICRC) have affirmed that existing international humanitarian law (IHL) is applicable to cyber operations in situations of armed conflict, the rules currently in place may be inadequate. Increased digitalization offers many advantages to humanitarian actors, but as the ongoing war in Ukraine demonstrates, there are a range of emerging risks, including the overlaps between civilian and military infrastructure, that put civilian networks in danger of attack. FP Analytics interviewed Dr. Peter Maurer, President of the Basel Institute on Governance and former President of the ICRC, about the challenges and opportunities related to upholding IHL in the age of hybrid warfare. The following transcript has been edited for length and clarity.

FP Analytics (FPA): How is the growing prevalence of cyber operations alongside kinetic warfare affecting humanitarian operations?

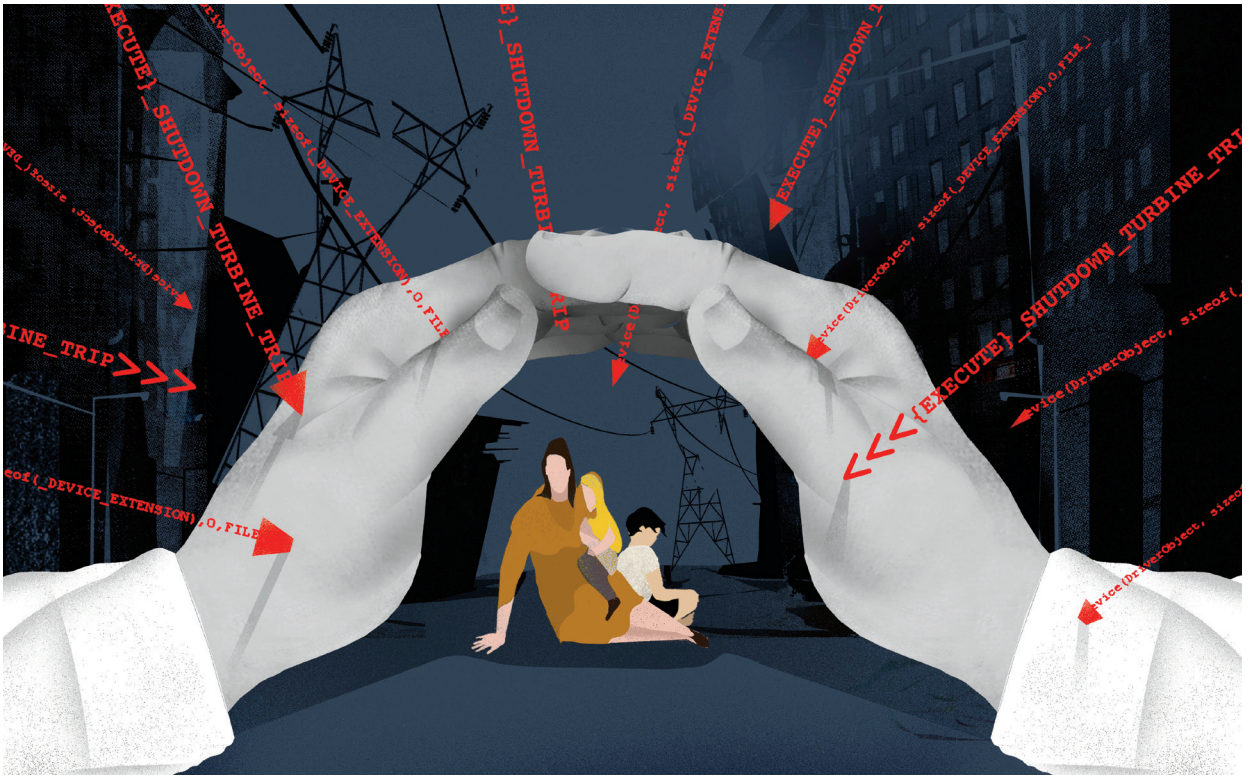
Dr. Peter Maurer (PM): The combination of kinetic and cyber operations is heavily affecting humanitarian actors. Cyber operations can cause collateral damage that affects cyber-based services to civilian populations. Humanitarian operators have increasingly gone digital, delivering digital services to people in terms of analytics and advice on where to go, where to find safe places, etc. Humanitarian agencies collect data on beneficiaries that are of interest to belligerents. They also conduct logistical operations that are heavily rooted in cyber support—making both humanitarian operations and civilian populations more vulnerable. Cyber-based misinformation, disinformation, and hate speech is also increasingly affecting civilian populations and humanitarian operations. The trust between beneficiaries of humanitarian aid and humanitarian organizations is shattered by misinformation and disinformation, as is the trust between governments and their populations. Also, the traditional categories like "What is the battlefield?" "Where is the battlefield?" "Where are military and civilian actors and humanitarian organizations?" have become fluid; battlefields enlarge and the technician doing the technical work on a cyberattack becomes eventually a direct participant in warfare even if his place of production is far away from the battlefield.

FPA: What are humanitarian organizations doing to improve their civilian protection efforts and safeguarding, and what more can they be doing?

PM: There are minimum precautions: education, training, beefing up your cybersecurity system as a humanitarian organization. Then there is, of course, technical know-how. Humanitarian organizations are not traditionally very digitally literate, but this can only reasonably be improved through partnerships with digital actors, companies, and specialists, which raises the dilemma of how neutral you can be depending on the partnerships. I have seen how important it is to have decentralized systems that are less vulnerable to attack than centralized cybersecurity systems. It is important to connect your operation to the people on the ground and raise awareness of the dangers of cyberattacks on civilians and humanitarian operators.

FPA: What can the international community do to better help humanitarian organizations in complex cyber contexts?

PM: The best support that a humanitarian organization can have from the international community is some minimal consensus on not attacking civilian populations and humanitarian organizations. For centuries, that has been the essence of humanitarian work. What states can do is develop best practices to instruct their militaries to not attack humanitarian and civilian organizations and populations.



Today, there are countries cognizant of the danger of intruding into a neutral humanitarian space via digital operations, countries that are instructing their military operators not to do so and to look for consensual arrangements with humanitarian organizations to deliver assistance. But this is not a norm at present.

FPA: Why is safeguarding critical infrastructure from cyberattacks so important for civilian protection? How does critical infrastructure fit into existing IHL?

PM: Attacks on critical infrastructure immediately lead to chain reactions and enormous vulnerabilities among populations. Countries that have already digitalized their public services become important entry points for humanitarian organizations. Let's take the example of Ukraine, which has developed its digital infrastructure over the past 10, 15 years enormously. Because of this, humanitarian responders were able, for instance, to deliver services to individuals affected by the conflict through existing digital infrastructure. What would have been goods on trucks delivered to people today can be transfers of cash onto cellphones and into the bank accounts of affected populations. It is also critically important that we build infrastructure that respects the principle of distinction in IHL between military and civilian infrastructure and actors.

FPA: How could IHL be adapted or expanded to encompass the challenges of cyber warfare?

PM: We need multiple strategies to adapt IHL to today's hybrid kinetic–cyber realities. The first entry point I would suggest is making logical legal interpretations from concepts that we have all agreed upon in the Geneva Conventions to make them applicable to cyber operations in today's conflicts. There are unquestionably gaps and a lack of clarity in IHL, so you need to do legal work to fill those gaps and create new norms or at least deliver manuals that instruct militaries on how to interpret IHL regarding cyber operations. I fully support the idea of a "digital Geneva Convention." The question is how fast we will be able to convince 196 state parties to agree.

FPA: Are there any other issues you feel are crucial to this topic?

PM: First, the concept of collective action, which is the effort among governments, the private sector, civil society, and the military to reach understandings over civilian protection. Second, there is no one body of law that will be applicable to hybrid warfare. We have to take into account human rights law, IHL, and eventually broader counterterrorism and terrorism legislation and consensus to find the best principles. Finally, there is an open question of whether artificial intelligence will help us find better processes and actions on the ground during conflicts. ■

Illustration by BRIAN STAUFFER

Tracing Cyberattacks in Times of Conflict: The Hard Path to Cyber Peace

Transparency and rigorous data collection are essential to credibly tracking cyber operations during the Russia-Ukraine war—as are being neutral and facilitating redress for all victims.

By STÉPHANE DUGUIN

CEO of the
CyberPeace Institute

Immediately following Russia's military invasion of Ukraine in February 2022, the CyberPeace Institute began tracking and analyzing cyber operations linked to the conflict. From the outset, it became evident that the invasion was going to lead us to question everything we knew about escalation in cyberspace.

Beyond our original purpose of tracking cyber operations to enforce accountability, continuous tracking has also given us a solid understanding of the technical and legal challenges associated with analyzing hybrid warfare. Over 16 months, the CyberPeace Institute documented and analyzed 1,998 cyberattacks and operations impacting 25 sectors in 50 countries. Through our online platform and quarterly reports, we have tracked the evolution of the threat landscape, the diversity of threat actors, and, most importantly, the human impact of attacks. We have tracked all types of cyber operations—from the crowdsourced distributed denial-of-service (DDoS) attacks to Viasat, the most sophisticated wiper campaign aimed at destroying infrastructure—and all types of actors, including those performing on behalf of Ukraine.

Since day one, the escalation has been concerning, not just because of the sheer statistical increase in the frequency and variety of attacks and the number of threat actors, but also because the military doctrines of both countries have evolved drastically. We have observed an increase in civilian and crowdsourced efforts alongside the continued presence of centralized and military incidents. Even so-called "hacktivist collectives" have played a significant role in the conflict. For example, the call for a volunteer IT army of Ukraine attracted civilian threat actors whose DDoS attacks have been heavily impacting Russian online resources. We have also documented the creation of various pro-Russian collectives, such as KillNet, People's CyberArmy, and NoName057(16), which target not only entities in Ukraine but also nonbelligerent countries. A significant number of NATO member countries that are not necessarily parties to the conflict have been impacted by cyberattacks carried out by hacktivist collectives—seemingly in response to those countries' public positions on geopolitical, ideological, or economic subjects.

CyberPeace has documented destructive cyberattacks aimed at the permanent deletion of data or rendering systems unrecoverable (e.g., the use of CaddyWiper or the ZeroWipe wiper). We have chronicled DDoS attacks targeting the availability of data or services. We have logged the proliferation of false information and propaganda through

> "Our role is to trace cyber operations so that attribution is properly documented and the data we gather is available for use as evidence. Key to performing a credible and neutral tracing of attacks are **transparency and solid data processing**."

defacement operations, and we have recorded incidents of data theft, followed in some cases by the leaking of that information to the public (i.e., hack-and-leak operations).

Tracing cyberattacks involves many challenges, one being attribution—discovering, calling out, and holding responsible parties accountable. Our role is to trace cyber operations so that attribution is properly documented and the data we gather is available for use as evidence. Key to performing a credible and neutral tracing of attacks are transparency and solid data processing.

Within the context of the ongoing Russia–Ukraine conflict, we made the decision to trace cyber operations everywhere. We collect data with the aim of facilitating justice and redressing all victims of cyber operations. Another challenge pertains to the participation of civilians in cyber warfare. How do states enforce plausible deniability or craft an attack to stay under the threshold of international law while crowdsourcing cyber operations?

And then there is the challenge surrounding recovery efforts. Should Ukraine win the ground war, it will not fully benefit from recovery efforts if its critical infrastructure—including its financial system and its information space—is not stable and secure and free from the presence of malicious actors. Recovery efforts must include a real digital ceasefire and support to clean malicious software from critical infrastructure and to protect the information space from propaganda and disinformation.

Since the invasion, we have learned that these challenges are so interlinked and complex that they cannot be addressed by one entity, organization, or country alone. As we believe that cyberspace is a digital public good, we maintain that tracing attacks, documenting attribution, and helping victims is the path toward accountability—and, hopefully, a de-escalation in cyberspace is a collective effort done for the greater good. ■

Illustration by MATT CHASE

Detect, Disrupt, Deter

The tech industry first pushed back against influence operations, malware developments, and espionage, but governments are catching up.

By DAVID AGRANOVICH

Director of Threat Disruption at Meta

Russian interference in the United States' 2016 elections fundamentally reshaped how internet platform companies approach security. In contrast to traditional content-moderation problems, influence operations like those we saw in 2016 were the work of networks of bad actors who deliberately abused product features to spread disinformation.

In the years since, several technology companies have adopted a model developed at Meta that goes beyond content moderation to integrate the detection of adversarial networks, the ability to disrupt their operations, and an information-sharing and disclosure regime designed to raise the cost to adversaries and reduce the impact of those operations. Since 2017, Meta's teams have disrupted more than 200 covert influence operations from more than 60 countries. This cadence of disruption has complicated the ability of Russian and other influence operations to develop mature platforms for influence and meaningful audiences to target. Each time we disrupt these operations, we use our discoveries to train machine-learning models on the bad actors' behaviors and detect them if they try to come back, and we re-engineer our products to make the terrain more challenging for adversaries. For example, after discovering in 2017 that Russia-based threat actors were using Facebook Pages to appear like American actors, our teams removed the deceptive pages and built tools to make the location of Pages administrators transparent, forcing bad actors to take substantial—and expensive—steps to evade detection.

As the technology industry has pushed back on these adversarial networks, they have evolved their tactics—becoming increasingly cross-platform and migrating to corners of the internet with more permissive (or nascent) moderation. In many cases, these operations fluidly cross between the online and offline worlds, relying on traditional intelligence techniques derived from pre-internet espionage—like the recruitment of third-party agents and the creation of forged documents—to enable their activity. And the perpetrators of these operations—once chiefly the domain of governments—are increasingly private for-hire companies operating as cyber mercenaries. These for-hire companies make it difficult for defenders to hold bad actors accountable, because the client behind the abusive activity is obscured. The evolution of these threats necessitates a whole-of-society approach to combat them. Larger platforms are getting better at identifying and disrupting bad actors, but meaningfully constraining their online activity requires cooperation across industry to raise defenses on smaller platforms that may currently lack trust and safety capabilities.

Governments, too, have an important role to play, as both defenders—by sharing actionable threat intelligence with the technology industry—and regulators. The growth of the for-hire disinformation and surveillance industries happened largely in a regulatory vacuum, with the strongest pushback on abusive spyware and disinformation-for-hire firms coming from private companies. Last December, Meta released detailed recommendations for governments to consider to more effectively constrain cyber mercenary actors, and there are heartening signs of progress.

Shortly after our report was released, Congress incorporated restrictions on for-hire surveillance procurement into the 2023 Intelligence Authorization Act and National Defense Authorization Act. In March, the White House released a landmark executive order restricting the U.S. government's procurement of commercial spyware and imposing further restrictions on its sale and use. This order coincided with an initiative by the Cyber Tech Accord, Microsoft, Meta, and others in the industry to formalize recommendations to constrain cyber mercenaries. The European Parliament's committee of inquiry on Pegasus spyware released detailed regulatory findings in 2023. There has not been a more opportune time for a multistakeholder approach: for industry, government, and civil society to push back against these threats together. ■

Developers Collaborate to Secure Software Ecosystem Amid Digital Threats

The war in Ukraine has shown that the tech industry has a meaningful role to play in enabling developers to strengthen defenses from cyberattacks.

By SHELLEY McKINLEY

Chief Legal Officer of GitHub

As modern warfare increasingly extends into the digital space, the global tech community has been playing an important role responding to, and building societal resilience against, hybrid threats. The Russian invasion of Ukraine has proved to be an inflection point for cyber operations, with developers on the digital front lines racing to strengthen defenses from cyberattacks. Home to more than 100 million developers, GitHub has had a front-row seat to these efforts.

Developers—even those in Ukraine directly affected by the war—have been using their skills not only to help with cyber defense and cybersecurity but also to supply the population with online tools. In the early days of the conflict, open-source developers vetted and aggregated information to build a heat map for tracking and avoiding war zones. Developers also built a centralized guide of border-crossing information that Ukrainians could reference to leave the country safely. As the Russian government's ongoing misinformation campaigns have intensified throughout the conflict, these types of resources have become increasingly valuable for Ukrainians seeking reliable information to protect themselves. Meanwhile, 100,000 tech workers left Russia in 2022 following the invasion, resulting in a large decrease in developer activity from Russia and large increases in such countries as Armenia, Georgia, and Turkey.

For developers, cybersecurity is a global collaboration to prevent and fix vulnerabilities before they can be exploited by cyber criminals. Attacks by state actors, particularly during war, put the security of the software ecosystem to the test and raise the stakes. Ukraine has been successful in mitigating damage to its cyber infrastructure because collective action across a broad spectrum of partners—in both government and industry—has given it an advantage in monitoring for threats and quickly identifying and patching vulnerabilities.

Software development services like GitHub provide platforms for developers to collaborate on securing the software ecosystem, including both proprietary software and open-source software that is free for anyone to use, modify, and share. Developers can leverage features that identify and scan code for weaknesses, alert them to patches for vulnerabilities, and use artificial intelligence tools with vulnerability-prevention systems. Companies like GitHub are also working across the industry with the Open Source Security Foundation to secure the entire supply chain and enable security researchers while thwarting active attacks. But beyond industry efforts, it is also important for governments to protect and support developers' security work, including by incentivizing vendors to take responsibility for the cybersecurity of their products.

The war in Ukraine has made it clearer than ever that the tech industry has a meaningful role to play in minimizing impacts of geopolitical conflict and supporting aid efforts. With more than 96 percent of the world's source code containing free and open-source software, it is important to protect open-source collaboration and the free flow of information across the global developer community. One crucial component of this is keeping software development services like GitHub open and available to developers—no matter where they reside—while complying with sanctions. Providing these services in countries that restrict internet access is essential for communications and humanitarian work as well as freedom of expression.

In an age of escalating cyber warfare, safeguarding the interconnected developer ecosystem is crucial to ensure the resilience, innovation, and collective defense needed to counter constantly evolving digital threats. ■

A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture

Responding to the growing threat of hostile cyber operations requires a mindset shift toward greater civilian–military cooperation as well as more engagement with the private sector.

By DAVID VAN WEEL

Assistant Secretary General for Emerging Security Challenges at NATO

Since 2014, Russia's cyberattacks against Ukraine have shown that malign actors won't hesitate to employ cyber operations—including disinformation campaigns, espionage, ransomware, and the crippling of essential services and critical infrastructure—at any time, up to and alongside combat operations.

But malign actors are not limited to Russia, and targets go beyond Ukraine.

The world is facing an era of long-term strategic competition. Little by little, malicious actors are interfering in our democratic processes and institutions and targeting the security of our citizens through hybrid tactics—both directly and through proxies. Understanding the role of cyberspace in strategic competition means understanding that there is constant friction and continuous activity in the cyber domain. In other words, cyberspace is contested at all times, not just during crisis and conflict.

Against this backdrop, effective defense in cyberspace means taking a more proactive approach. This requires a shift away from the mentality of relying exclusively on deterrence by denial—persuading an adversary not to attack by convincing it that an attack will not achieve its intended goal. Instead, we need to foster an entirely new mindset regarding how to operate, compete, and, if necessary, fight in the cyber domain.

The first step is to embrace a comprehensive approach to cyber defense. This requires a better integration of activities among numerous stakeholders at each of NATO's three cyber defense levels—political, military, and technical. At the political level, we need to be proactive to shape cyberspace in line with our values, promote stability through forward-looking policy development and the support of international norms, and clearly signal to adversaries that we are prepared to respond swiftly. At the military level, we must strengthen the role of our military cyber defenders by enabling civil–military cooperation throughout peacetime, crisis, and conflict. At the technical level, we must strive to defend ourselves effectively, ensuring that we are well equipped to detect, prevent, and protect against malicious cyber activity.

Second, effective national defense requires acting coherently with other states and relevant actors. We are stronger together in defending our values, and we cannot afford to duplicate our efforts. NATO offers a platform for political consultation and collective action against cyber and hybrid threats. Addressing the need to meet the current cyber threat landscape head-on, allies endorsed a new concept at the Vilnius summit to enhance the contribution of cyber defense to NATO's overall deterrence and defense posture. As a result, NATO will further develop

> "Effective national defense requires acting coherently with other states and relevant actors. **We are stronger together in defending our values**, and we cannot afford to duplicate our efforts."

and enable civilian–military cooperation throughout peacetime, crisis, and conflict. Recognizing the unprecedented and critical role the private sector has played defending Ukraine from cyberattacks, another key focus of the concept will be strengthening the integration of industry expertise, as appropriate, in order to better protect NATO and allied networks, operate in cyberspace, and shape cyberspace in line with our values.

Beyond industry cooperation, NATO continues to intensify its cooperation through partnerships, including with partner countries, academia, the private sector, and other international organizations. For example, NATO cooperates with the European Union through a Technical Arrangement on Cyber Defence and continues to strengthen cooperation on cyber defense with efforts including information exchanges and training exercises.

Third, we must not forget the critical importance of resilience in cyberspace—getting the basics right and ensuring that defenders have the capabilities to detect, prevent, and mitigate malicious activity. Resilience is a cornerstone of cyber defense's contribution to NATO's overall deterrence and defense posture. Beyond endorsing the new concept, at Vilnius, allies also agreed to new and more ambitious national cyber defense goals and minimum requirements as part of the enhanced Cyber Defence Pledge, which recognizes that as states strengthen their defenses, they raise the cost to adversaries. While we may never be able to prevent all cyber incidents, we certainly will not succeed by sitting back and waiting for something to happen. While strategic competitors try to exploit NATO's fault lines, the story of Ukraine's defensive successes in cyberspace has demonstrated the power of having an effective cyber defense posture.

Finally, this new concept recognizes that being proactive cyber defenders also means being responsible actors. Beyond respecting our international commitments to upholding a norms-based approach to responsible state behavior in cyberspace, NATO allies and partners must be prepared to uphold the values and principles that drive us. We must be bold in enforcing norms. This will involve using all the tools in our democratic toolbox, ensuring over time that we not only raise the cost to malign actors but also hold them accountable when norms are being broken.

Any adequate response to these strategic challenges requires a genuine ambition to coordinate cyber defense efforts effectively. And it must be so. Just as we see constant friction in cyberspace, our cooperation should be always present—between allies, across the civilian–military spectrum, and between public actors and industry. ■

Illustration by MATT CHASE

Strategies to Deter and Respond to Cyber Operations in Conflict

International cooperation is integral to solve key challenges and reduce socioeconomic and geopolitical risks.

The integration of cyber operations with kinetic warfare, including the alarming scope of cyberattacks on civilian and military targets since Russia's full-scale invasion of Ukraine, represents the latest troubling development in armed conflict. While we cannot predict precisely how digital technologies may be weaponized in the future, the international community today faces an urgent, complex challenge: identifying how to bolster cyber defense strategies and best regulate and respond to cyber operations in the lead-up to or alongside military operations.

This final issue brief brings a sharpened focus on matters that need to be addressed through multisector collaboration, including how cyber operations in contemporary armed conflicts are challenging rules of engagement and lessons that can be drawn from existing approaches to risk mitigation for dual-use technologies to help ensure international stability.

Illustration by KLAWE RZECZY

Three key insights emerge from this analysis. First, cyberattacks on critical infrastructure not only threaten civilians' safety but also impose significant socioeconomic costs and require greater public–private partnerships to deter reckless behavior online and uphold a rules-based international system. Second, it is critical to clarify how international law applies to cyber operations surrounding armed conflicts. Finally, coordinated and complementary action by governments, multilateral institutions, tech companies, academia, and civil society will be crucial to developing strategies for defending against the destructive impacts of hybrid warfare.

Protecting Civilians and Infrastructure from Cyber Operations Through International Law

Both independently of and in combination with kinetic attacks, critical infrastructure has become a recurring target in hybrid warfare. The digitalization of operations systems has exposed new vulnerabilities while states have pursued disparate approaches to attribution and accountability in the aftermath of a cyberattack on critical infrastructure. Among cyberattacks carried out by state-affiliated actors globally, the share on critical infrastructure increased from 20 percent to 40 percent between 2021 and 2022. In 2022, for example, amid growing geopolitical tensions and proxy warfare, an Iran-linked group targeted the network of an Israeli logistics company, causing a system shutdown and disrupting the company's supply chain operations. These types of attacks are unlikely to abate soon: The World Economic Forum's *Global Risks Report 2023* projects that cyberattacks on key sectors will only become more prevalent. And because critical infrastructure sectors are largely interdependent, an attack on a power grid, for example, can have magnifying effects, disrupting other vital sectors such as communications and health care. Such cyber operations heighten not only the risk to public safety but also the potential for kinetic retaliation or escalation of conflict amid worsening political tensions.

The widespread and complex impacts of hybrid warfare underscore the need to identify effective cybersecurity and deterrence strategies as well as defined pathways for legal recourse. To that end, encouraging progress is being made: In 2021, United Nations member states agreed to the principle that international humanitarian law is applicable to cyberattacks during armed conflict. Member states also adopted the norms recommended by an Open-ended Working Group reaffirming the need to safeguard critical infrastructure at all times, including peacetime, such as by improving the cybersecurity of infrastructure operating systems. There is much more to be done, particularly as chemical, biological, radiological, and nuclear materials and capabilities—as well as outer space assets—are increasingly managed and monitored digitally, heightening their vulnerability to cyberattack or cooptation.

In situations of armed conflict, there is growing acceptance that state-affiliated cyber operations that cause physical damage could be classified as "armed attacks" under international law. Such "armed attacks" would then be covered by the same established international legal regime that regulates kinetic operations, like missile strikes. Despite this emerging consensus, the nature of cyberspace can blur the distinction between civilian and military targets and complicate the protection of civilians from attacks by warring parties, which is enshrined in international humanitarian law (IHL). Much of the infrastructure of the internet, for example, serves both civilian and military users and is a key site of economic activity. Unless IHL on this point is clarified, attacks on civil–military infrastructure could be deemed justified by some actors, despite negative impacts on civilians.

Like nuclear assets, cyber technologies that can be used as weapons can also be powerful tools for improving lives. Considering their dual use, cyber technologies warrant carefully crafted normative and legal responses, rather than blanket bans, to enable their beneficial uses while limiting their destructive potential. The establishment of an international body similar in function to the International Atomic Energy Agency could provide oversight and investigation to promote the safe use of cyber capabilities. Similarly, the U.N. Secretary-General recommended in his July 2023 policy brief on "A New Agenda for Peace" the creation of a multilateral mechanism for

National and Multilateral Bodies Have Been Working to Regulate Cyberspace for Two Decades

Despite increased attention paid to cyber operations and their impacts, applicability of international law to cyber remains vague and unclear.

1999

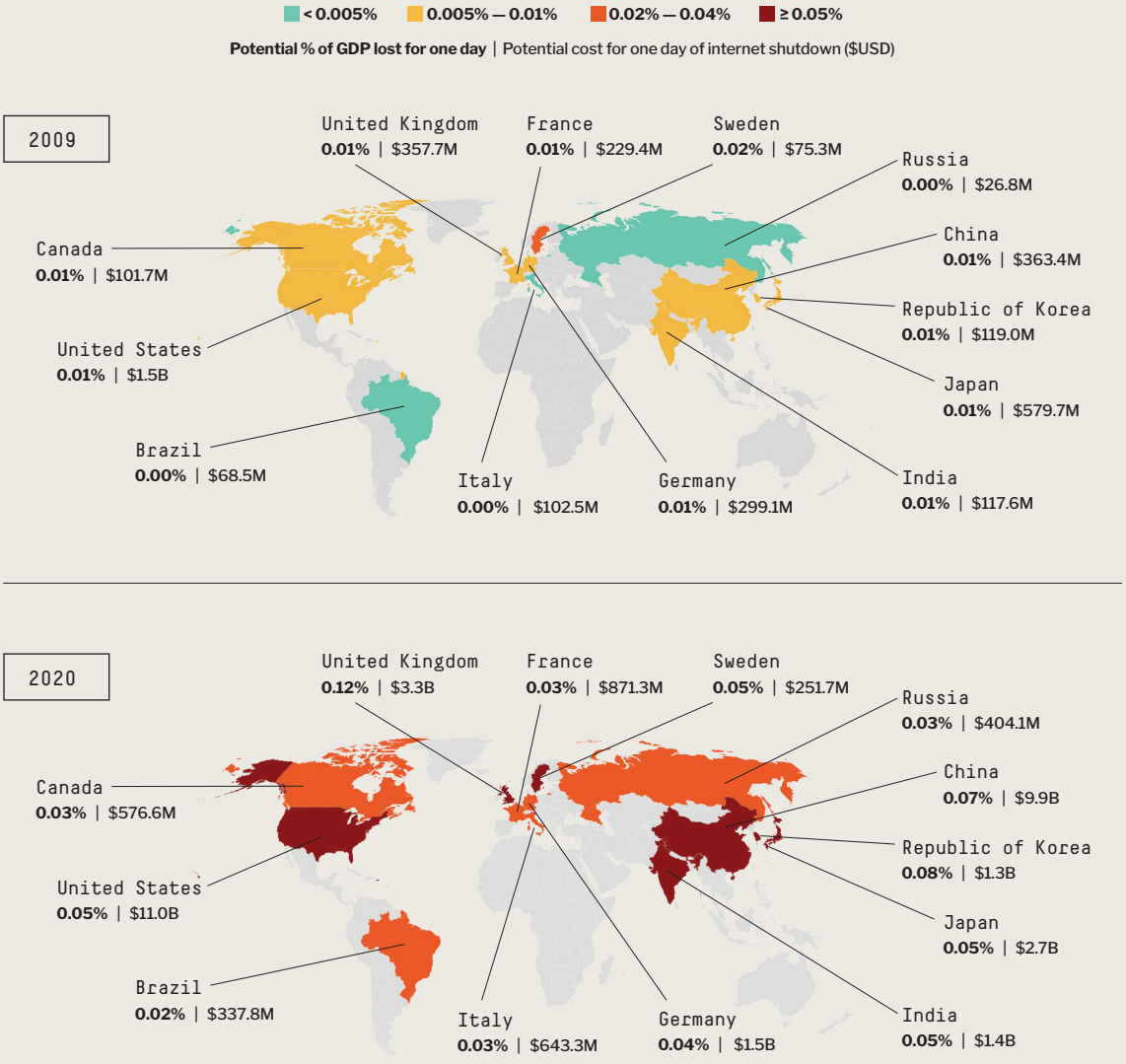
U.S. Naval War College convenes first major legal conference on cyber operations.

2004

The first U.N. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security is convened.

A Cyberattack Could Cost Economies Billions

As the digitalization of jobs and services has increased, so has the world's vulnerability to an attack that shuts down the internet.



Data sources: NetBlocks, Brookings Institution, McKinsey, World Development Indicators

2010
The U.S. and U.K. national security strategies cite cyber threats as one of the most serious national security challenges to their nations.

2010
The United States establishes U.S. Cyber Command.

2010
NATO acknowledges cyber threats in 2010 Strategic Concept.

2011
The U.S. Department of Defense issues Strategy for Operating in Cyberspace, designating cyberspace as an operational domain.

2011
Russia releases a cyber concept for the armed forces: Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space.

accountability to address malicious cyber activity. Relatedly, while artificial intelligence is still in the early stages of regulation and international governance, there is much to be learned from recent attempts to encourage its responsible development, such as the U.S. State Department's 2023 Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy. Another domain of dual-use technology from which lessons can be drawn and applied is outer space, where—similar to the cyber realm—international consensus and governance are complicated by the presence of an increasing number of both public- and private-sector operators engaged in activities that span the military and commercial spheres. As regulations, laws, and norms are developed, it is vital that technical experts, policymakers, and industry leaders take into account—and build resilience against—cyberattacks, which pose a threat across these areas of dual-use technology.

Mitigating Damage and Escalation with Clear Standards and Norms on Attribution

In addition to the debate around the protection of civilians and civilian infrastructure, there is a need to reach consensus around accepted norms of behavior and response in the event of a state-perpetrated cyberattack. Currently, with no clearly defined international legal and governance process in place, states wishing to retaliate against a cyberattack are responsible for provable attribution, which is sufficiently challenging to sometimes allow aggressors to act with impunity. For example, while the United Kingdom attributed the 2017 WannaCry malware attack to North Korea within weeks, it took seven months for the U.S., New Zealand, Canada, and Australia to concur. Demonstrating the lack of guidance around attribution, none of these five countries publicly presented evidence for their claims. In response to this general lack of clarity, experts have proposed various guidelines—for example, a U.N. Group of Governmental Experts' 2015 recommendations and the Organization for Security and Co-operation in Europe's 2016 compilation of best practices. However, these proposals have yet to be widely reflected in public attribution statements.

Establishing standards for evidence is further complicated by the difference in process for technical versus political attribution: While the former is relatively straightforward, using digital forensic tools to ascertain what software and hardware was used in an attack, the latter is more challenging, as states often use cyber mercenaries and other proxy actors to perpetrate attacks while maintaining plausible deniability. An approximately $12 billion industry, cyber mercenary services have been used by at least 74 governments since 2011. More recently, governments have begun to take action on cyber mercenaries, with 36 member states of the Freedom Online Coalition developing and signing the Guiding Principles on Government Use of Surveillance Technologies, which launched in 2023. These principles seek to delineate the lawful use of cyber mercenaries by governments to protect human rights and privacy. Guidance includes implementing clear and transparent processes for decision-making regarding digital surveillance and providing access to ongoing legal training for all government employees involved in these processes.

Multilaterally, NATO's updated cyber defense posture—announced during the July 2023 Vilnius summit—may provide a model for enhanced cybersecurity in the face of rapid change. The announcement included calls for allies to regularly update their own cyber-related strategies and laws and a commitment to better civil–military cooperation on cybersecurity, including during peacetime. These initiatives and recommendations, while promising, still fall short of a universal consensus let alone binding international laws. These are crucial areas that need to be explored by future collaborations among stakeholders, including multilateral institutions, civil society organizations, tech companies, and states.

Collaborating Across Sectors: States, Industry, Civil Society, and Academia

The use of cyber operations in armed conflict calls for an international

2013
Publication of the non-legally binding *Tallinn Manual on the International Law Applicable to Cyber Warfare.*

2013
NATO CCDCOE launches initiative to expand *Tallinn Manual*'s scope to include cyber operations during peacetime.

2013
NATO CCDCOE convenes new International Group of Experts to adopt additional rules for peacetime cyber activities.

2013
U.N. Group of Governmental Experts recognizes the applicability of existing international law to information and communications technology (ICT).

2014
The African Union adopts the Malabo Convention on Cyber Security and Personal Data Protection.

system with agile multilateral institutions able to adapt in the face of new developments and capable of engaging with academia and nongovernmental organizations, as well as the private sector. Amid what has been dubbed a "new digital order"—as established power dynamics among nations shift based on their access to and use of cyber capabilities—tech companies are playing a growing role in detecting and defending against cyberattacks, as they own and operate much of cyberspace. Finding themselves on the digital front lines of conflict, more than 150 tech companies have become signatories to the Cybersecurity Tech Accord since its 2018 launch, providing a corresponding voice for the industry on matters of peace and security online, including the use of cyber mercenaries and digital surveillance.

The act of detecting and responding to national security threats, such as the China-linked 2023 hacking of U.S. government email accounts, warrants close collaborations across the public sector, NGOs, and private companies. One strategic opportunity for cooperation is cybersecurity workforce development; the inclusion of diverse voices and expertise across government, industry, academia, and civil society can not only strengthen technical know-how but also establish broad-based support for future approaches. As the evolution of new cyber threats and information operations outpaces existing digital infrastructure and security protocol, "expertise gaps" expose critical vulnerabilities. Additionally, the global demand for employees in cybersecurity outpaced supply by 3.4 million workers in 2022, with the widening gap attributed to a lack of interest, diversity, and skills in the pipeline, and high barriers to entry.

To address these challenges and in the interest of international security, educational institutions, the tech industry, NGOs, and the public sector can pursue various strategies to improve the workforce and strengthen cyber resilience. These include developing foundational digital skills among young people and traditionally underrepresented groups, reskilling the non-cybersecurity workforce, establishing trusted accreditation, and incorporating digital literacy and cybersecurity into the training of defense, diplomatic, and multilateral professionals. Lessons learned from past technological transitions can be leveraged to prepare for the possibility of future cyber-integrated hybrid warfare across all sectors and industries, and would benefit from the expertise and resources of various stakeholders, including international financial institutions, trade and development organizations, and global infrastructure investors and insurers.

Pursuing Cyber Peace and Preparing for Potential Cyber Conflict

The emergence and integration of cyber operations into warfare and conflict has brought to the fore challenges to international governance and stability, but it has also amplified existing issues and underlying tensions that threaten to undermine global peace and prosperity.

These issues will change over time as technology evolves, new uses for cyber capabilities emerge, and theaters of war expand. Institutions therefore need to focus on creating, expanding, and clarifying regulations, norms, and international humanitarian laws so that they can grow and adapt as technology does, or risk becoming outdated and obsolete.

A whole-of-society approach is needed to anticipate, mitigate, and address potentially catastrophic risks to critical infrastructure, human security, and the global economy. To help meet this challenge, the public and private sectors need to scale their partnerships, invest in minimizing vulnerabilities in cybersecurity, and develop a high-skilled cyber workforce. Creative collaborations, in the spirit of the Digital Front Lines project, can bring together experts from across the spectrum—cyber, international humanitarian law, diplomacy, the military, civil society, and more—to envision what a stable, peaceful future looks like in the digital era. ■

By Angeli Juani (Senior Policy and Quantitative Analyst), Avery Parsons Grayson (Senior Policy and Research Analyst), Isabel Schmidt (Senior Policy and Research Analyst), and Dr. Mayesha Alam (Vice President of Research).

Timeline sources: U.S. Cyber Command, Tallinn Manual, Tallinn Manual 2.0, Carnegie Endowment for International Peace, Council of Europe, Lawfire, U.N. General Assembly, United Nations Office for Disarmament Affairs, Digital Watch, African Union, People's Republic of China State Council

2016
China releases its first National Cybersecurity Strategy.

2017
The *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* is published.

2018
The U.N. General Assembly adopts resolution on "Advancing responsible State behaviour in cyberspace in the context of international security."

2020
UNGA creates Open-ended Working Group 2021–2025 on ICT to develop rules, norms, and principles related to cyberspace.

2022
The EU Council introduces a framework for a coordinated EU response to hybrid campaigns.

U.N. Responsibilities in the Digital Age

A Q&A with
IZUMI NAKAMITSU

U.N. Under-Secretary-General and High Representative for Disarmament Affairs

Speaking to FP Analytics, U.N. Under-Secretary-General and High Representative for Disarmament Affairs Izumi Nakamitsu outlined the challenges posed by malicious cyber activity to international peace and security and the steps the United Nations is taking to adapt to the evolving nature of conflict in the digital age. The following transcript has been edited for clarity and length.

FP Analytics (FPA): What are currently the top concerns and priorities of the United Nations Office for Disarmament Affairs when it comes to cyberspace?
Under-Secretary-General Izumi Nakamitsu (IN): I think we are witnessing unprecedented challenges to the peace and security of cyberspace, including in connection with the war in Ukraine. We are witnessing how malicious activity in this domain can be used to support active hostilities, and we are looking at the broad trends, including the increasing number of incidents affecting critical infrastructure and other sectors that provide services to the public. We are also concerned about malicious criminal activities in cyberspace. All of these malicious activities are starting to impact people's daily lives. That's one of the main concerns driving our work to deepen multilateral dialogues to strengthen common norms, rules, and principles and ensure their effective implementation.

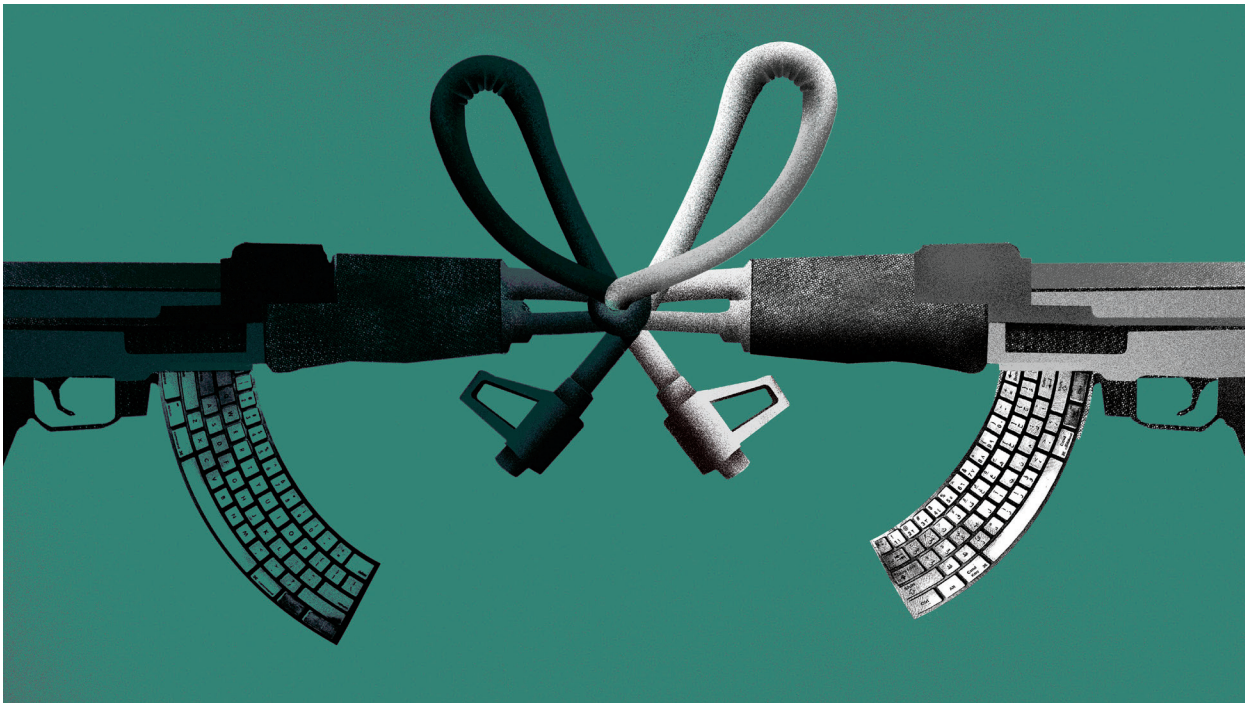
FPA: How can the U.N. work with member states to foster a culture of accountability and adherence to norms, rules, and principles in cyberspace?
IN: The U.N., in particular my office, is primarily tasked with supporting intergovernmental discussions on matters related to cybersecurity in the context of international security. We continue to work hand in hand with member states in this regard, including the chair—the ambassador of Singapore—of the ongoing Open-ended Working Group on the security of information and communication technologies. In this working group, states are discussing critical issues related to strengthening norms, advancing confidence building, unpacking the applicability of international law to cyberspace, and enhancing capacity building.

The U.N. also continues to support multistakeholder engagements in this area. Because of the unique nature of cybersecurity and cyberspace itself, various actors from civil society, industry, the private sector, and academia need to play a role in the advancement of responsible behavior in the cyber domain and the implementation of confidence-building and capacity-building initiatives. The inputs from these actors are essential for effective cybersecurity responses.

The secretary-general also continues to lend his voice to the call to prevent the escalation and extension of conflict and hostilities into cyberspace and does so again in his new policy brief, "A New Agenda for Peace."

FPA: What are the issues policymakers should consider when forming laws, policies, and practices regarding cyberspace, cyber warfare, and cybersecurity?
IN: Challenges to the peace and security of cyberspace can only be expected to grow. Responding to and mitigating risks emanating from cyberspace have become, rightly so, top-line priorities. I am particularly concerned about how to protect critical infrastructure that provides essential services to the public—for example, water and sanitation, energy, telecommunications, and transportation. It is also important to ensure that governments have the capacity at the national level to implement the already agreed-upon norms of responsible state behavior. We also need to discuss what confidence-building measures in cyberspace might look like. What are the measures that governments can take to de-escalate tensions and disputes in cyberspace? And we must further unpack how international law applies to cyberspace and continue discussions related to accountability. The issues are wide-ranging, and intergovernmental discussions are progressing, but we must continue to see steady progress.

Amid an international security environment under enormous strain, moments like this demonstrate the necessity of common norms, rules, and principles. We must make sure we collaborate with governments, civil society, and the private sector so that states make progress on these issues, not despite the current environment but because of it.



"It is key that we are always guided by humanitarian principles, no matter the domain."

FPA: What could cyber disarmament look like? Could we ban certain technologies for use in conflicts, or should we?

IN: First, I think it's important to underscore that there are no such things as "cyber weapons." In addressing cybersecurity, it is not about categorizing a specific "weapon." Information and communications technologies are enabling technologies and can be dual-use or multipurpose. Rather than trying to figure out how to regulate and ban the technologies themselves, we should focus on responsible use of these technologies and unpack questions related to the applicability of international law and accountability. Twenty-first century arms control and disarmament discussions, including those related to cyberspace, will very likely require a combination of various multistakeholder initiatives, including some initiated and led by the private sector. Good examples of such initiatives in the cyber realm are the Cybersecurity Tech Accord led by Microsoft and the 2018 Paris Call for Trust and Security in Cyberspace. In addition to intergovernmental negotiations on something that will bind states, we should pay attention to interesting approaches like these. Governments, academia, and civil society are now coming together to seek solutions, and this will start to have a real impact, I hope. One key issue, of course, is accountability—how to make sure those norms and principles are adhered to.

FPA: Cyber conflict can blur the lines between civilians and combatants. How are you thinking about this challenge, and what is the role of the U.N. in clarifying or maintaining those boundaries going forward?

IN: This is one of the most important and difficult questions we are faced with. If civilian entities are involved in offensive actions in cyberspace, would they be considered combatants or civilians? This is why the intergovernmental discussions at the United Nations need to get down to the details of how international law, including international humanitarian law, applies in cyberspace. It is key that we are always guided by humanitarian principles, no matter the domain.

FPA: What are the open questions that need to be addressed regarding the future of cyber warfare?

IN: Most urgently, there is an acute need for protecting critical infrastructure. Secondly, it is vital to enhance accountability in relation to the spread of mis- and disinformation. There is also an urgent need for cybersecurity capacity building to support states in implementing their commitments. And, finally, among the most difficult but still essential issues is further unpacking the applicability of international law. ■

Illustration by BRIAN STAUFFER

How Russia Makes Friends and Influences Audiences in Latin America

Russia's success in establishing and maintaining a media foothold in Latin America highlights how important worldwide influence campaigns are to hybrid warfare.

By CLINT WATTS

General Manager of the Microsoft Threat Analysis Center

The power of influence operations and well-funded state-sponsored propaganda outlets have been of central importance to Russia during its hybrid war in Ukraine. Influence operations have often complemented both military action on the ground and cyberattacks in an attempt to deepen divisions in societies supportive of Kyiv, shape perceptions among otherwise nonaligned audiences, and reinforce the Kremlin's strategic objectives worldwide.

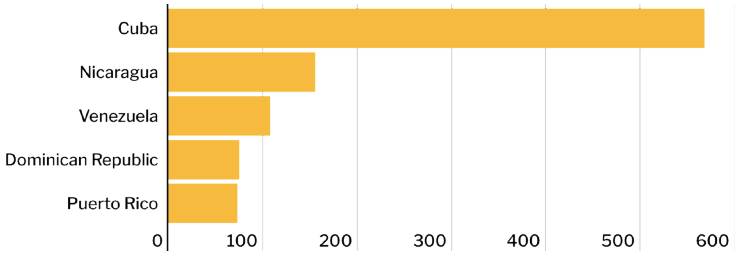
Over the past year, analysts and observers have—justifiably—focused most on Russia's malign activity on the battlefield, online, and in the information space in Europe. However, as we forecast the future of hybrid warfare with global impacts, we should be aware of influence activities that the Kremlin continues to conduct in geographies and languages further afield. In Africa and the Arab world, for example, Russia's multifaceted operations continue apace, relying on both overt and covert means, online and off, to achieve its geostrategic aims of promoting Russia's international image and cultivating economic and political leverage in the region.

In Latin America, Russia has sought to reach local audiences primarily through its state-sponsored media arms and their attendant social media presences. While Latin America has been a focus for Russia's media strategy for more than a decade, recent flashpoints—and what appears to be increasing success in landing messages and shaping discourse—highlight the importance of understanding the mechanisms through which an audience from any part of the globe might be influenced through local coverage.

Russia's influence approach to Latin America relies heavily on its overt media properties, led chiefly by RT en Español, the Spanish-language arm of Russia Today that launched in 2009. In recent years, the network has claimed a live television audience of 18 million in Latin America, while the outlet's following across several social media platforms surpasses Spanish-language offerings from international competitors such as the BBC and CNN. Audience figures are further buttressed by deals signed with more than 1,000 regional satellite TV providers to carry RT, 33 correspondents based throughout Central and South America, and the distribution of RT via media in Cuba, Nicaragua, and Venezuela, where state-affiliated outlets maintain broadcasting agreements with Russian state media. RT has been given further legitimacy by political figures who readily appear on—or even work for—the network. The breadth of these networks enables Russian state-sponsored media to reach audiences with coverage on flashpoints or international

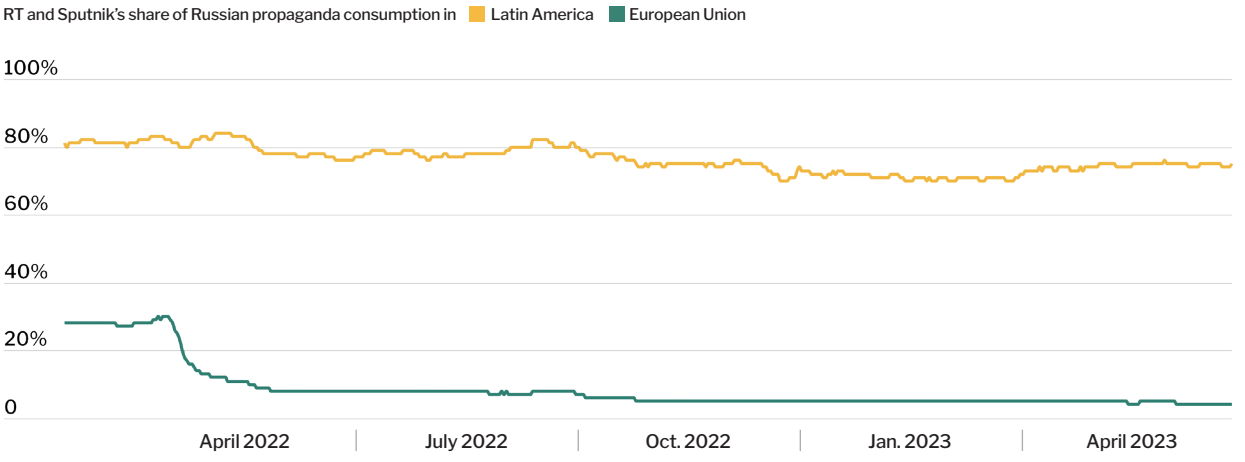
Russian Propaganda Index Shows State Media's Widespread Influence in Latin American Nations

The RPI measures the proportion of propaganda flow to overall news traffic on the internet; these measures represent Jan. 1 to May 10, 2023.



While RT and Sputnik's Footprint has Diminished in the European Union, It Remains High in Latin America

The two media outlets account for a large share of Latin America's Russian propaganda consumption.



Data source: Microsoft AI For Good Lab

events deemed either out of scope or too expensive for major domestic Latin American media outlets to cover.

RT's coverage is widely consumed in the region. Microsoft's AI for Good Lab developed a Russian Propaganda Index (RPI) that monitors via Microsoft telemetry the flow of news from Russian state-controlled and state-sponsored news outlets and amplifiers. This index measures the proportion of propaganda flow to overall news traffic on the internet. An examination of RPI figures from the first four and a half months of 2023 confirmed that Cuba, Nicaragua, and Venezuela—to which the Kremlin's preferred narratives are consistently distributed and amplified among local audiences—have the highest levels of Russian propaganda consumption in Latin America, with the Dominican Republic and the U.S. territory of Puerto Rico following closely behind.

Coverage of Local vs. International Events

Russia's spin on local events can be seen most readily in its coverage of European and U.S. officials' visits to the region: In one case, Russian state-sponsored media aggressively framed a routine visit as an "imperialist" quest to procure lithium—two-thirds of the proven reserves of which are in Latin America—for electric cars and military equipment. Mischaracterizing and misquoting officials, RT's reporting often focuses on negative local sentiment, even when this represents a minority view. Efforts to cover local news have been partially responsible for RT's and Sputnik's substantial regional footprint. RT accounts for 51 percent of all Russian propaganda consumption in Latin America and is the most visited Russian propaganda site in every Spanish-speaking nation. Sputnik, meanwhile, accounts for an additional 23 percent of Russian propaganda consumption in Latin America, with more than 90 percent of its traffic coming from the Spanish-language Sputnik Mundo and the Portuguese-language Sputnik Brasil.

These two sites have remained the most visited Russian propaganda sites in Latin America while traffic originating from many Western countries to them dropped after RT faced sanctions following the February 2022 full-scale invasion of Ukraine. After the EU suspended their broadcasting rights, observed traffic to RT and Sputnik consumption dropped by upward of 80 percent in the EU.

Looking Forward

Notwithstanding legitimate concerns about overstating the effectiveness of Russian propaganda in the global south, the fact remains that Russia has placed a large bet on a top-down strategy in Latin America. With overt state media leading a multipronged strategy, Russia's influence apparatus has proved successful insofar as RT and Sputnik have maintained a consistent audience share despite the downward pressures of sanctions and online moderation of state propaganda outlets during the war in Ukraine.

To respond to the new era of hybrid threats emanating from Moscow—which align kinetic, cyber, and influence activities for greater effect—states should not only harden their network infrastructure but should also promote resilience in the information space. Part and parcel of this agenda is understanding the extent and efficacy of Russian propaganda in nations around the world. ■

A Multisector Approach to Tackling the Threats of Emerging Technologies on Defense Systems

A Q&A with AMBASSADOR BONNIE JENKINS

U.S. Under Secretary of State for Arms Control and International Security

Speaking to FP Analytics, U.S. Under Secretary of State for Arms Control and International Security Bonnie Jenkins discussed how emerging and disruptive technologies require new approaches to address potential threats to international security. The following transcript has been edited for clarity and length.

FP Analytics (FPA): What are the main challenges to security and deterrence in chemical, biological, radiological, and nuclear defense with regard to cyberattacks?

Ambassador Bonnie Jenkins (BJ): The main issue right now is trying to gain a sense of how cyberattacks affect planning and execution in the military. We have seen the increased use of cyberattacks as well as cyber expertise in the past few years. We need to continue to understand how we can address cyber situations that impact our national security. To that end, we have set up entities within the U.S. government that focus on our defensive and offensive capabilities.

FPA: How do you think advancements in artificial intelligence (AI) complicate these dynamics?

BJ: First of all, there are a lot of positives to AI. There are a lot of things that can be done in terms of arms control, and there may be ways we can use AI to improve the verification of treaties, the verification of many types of risk-reduction efforts.

But, of course, there are also things we need to worry about. How do we make sure AI is being used responsibly? AI, like other emerging technologies, is developing so fast. In many ways, governments are behind the curve. There are so many entities that are involved: not just government, obviously, and not just the military, but industry and academia.

We don't know what AI or any emerging technology is going to look like a year from now, so we need to have some way to responsibly address this technology, particularly in the military sense. When we talk about space, for example, the U.S. has tried to get countries to agree not to do direct-ascent anti-satellite weapons tests, which the Russians did a couple of years ago and left a lot of debris in the atmosphere. And, fortunately, we were able to, at the U.N. General Assembly, get 155 countries to agree to that.

We took this concept of responsible behavior in emerging technologies, and in February 2023, I was able to announce at a summit in the Netherlands the Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy. What the declaration sets forth are a number of principles for countries to adopt in terms of AI and the military, such as ethical issues about developing technologies.

We are also looking at making sure a human is involved in any nuclear decision-making. We are working with countries in all regions of the world to develop guardrails and determine how to be responsible in these areas. But it is going to be important not just for government but for industry to also be involved.

FPA: What is the role of the private sector in safeguarding weapons systems and related infrastructure?

BJ: It is important to recognize what the private sector can provide us. They're out there working on these technologies, developing them in many parts of the world. These are opportunities for us in the government to really see the cutting-edge work that's going on, involve them in these discussions, and learn from their expertise.

They may already be doing things we want to do, so there's no reason for us to duplicate that work. We do need to stay abreast of who is involved and what they are working on. How can we work hand in hand with them on these emerging technology issues? Unlike many of the ways we've done traditional arms control in the past, this is an area where we really do have to be working with industry, because so much is happening outside government and in academia, where they're doing a lot of exploration on emerging technologies.

FPA: Can you explain how arms control now is different from how it was in the past?

Illustration by BRIAN STAUFFER

BJ: For many years, we were trying to promote predictability in the international system when it comes to chemical, biological, nuclear weapons. And we did so by negotiating and concluding a number of treaties—the Nuclear Non-Proliferation Treaty, Biological Weapons Convention, Chemical Weapons Convention, the New START Treaty that we have with Russia, etc. These are all ways that, under international law, regulate, disarm, and promote the nonproliferation of these weapons. Emerging technologies have provided a different requirement in how we address what can create instability in the international system. And some of these actions do not necessarily fit the traditional arms control way of doing things.

New challenges posed by emerging technologies demand another way of looking at how we promote predictability in an international system. So there is the traditional way we've done arms control, with legally binding treaties that go to the Senate for advice and consent. But there are also things we can do to develop risk reduction, crisis management, confidence-building measures and norms—ways in which we work with other countries to take activities that provide some predictability and reduce miscalculation to ensure we don't do things that will create instability in the international system.

FPA: Are there any promising public-private partnerships that can inform efforts going forward?
BJ: The Arms Control, Verification, and Compliance Bureau is actually working with some academic institutions—for example, the University of Maryland—to get a better understanding of what they are doing on emerging technologies and ways the government can collaborate. We also have something called a Verification Fund where we provide funding to entities that have innovative ideas regarding verification and the use of these technologies.

FPA: What might the structure and content of expanded or adjusted agreements tailored to current cyber realities look like?
BJ: We don't really know what all the threats might be because we are still learning about the opportunities and challenges that stem from emerging technologies. We have to come to the table discussing these issues with many unknowns but still needing to consider how to approach these new areas. We also have many actors in these fields. We have industry, research institutes, and academia, in addition to many government actors. This unique situation will lead to a different approach in a new landscape.

FPA: What insights can be derived from Russian threats to nuclear zones in Ukraine—most notably the Zaporizhzhia Nuclear Power Station—and how can these insights be applied to safeguarding nuclear facilities worldwide?
BJ: We need to have more ways of looking at how we approach the safety and security of these kind of plants. One of the things that the International Atomic Energy Agency did, led by Director General Rafael Grossi, was to develop principles that countries should agree to with regard to safety and security in times of conflict. And the thought process behind these principles is that you're talking about nuclear safety, nuclear security issues, things that if abused could lead to significant damage to countries. We recognize that we need to think about nuclear safety in times of war and nuclear security in times of war. And while we assumed that there's a recognition among countries that taking over a nuclear power plant and bombing areas around the plant are not good things to do, maybe we need to develop more principles in terms of parameters for dealing with these kinds of situations and conflicts. Hence the principles.

FPA: What are your top priorities for increasing cybersecurity around chemical, biological, radiological, and nuclear defense?
BJ: I think we have to find ways to constantly stay ahead of countries or other entities that want to use cyber in ways that can be even more devastating in terms of weapons of mass destruction. Cyber can be used in a way that brings great challenges in terms of financial risk and personal information. However, when you're talking about cyber in terms of nuclear, chemical, or biological weapons, the potential risks to the international community are even more grave. So, I think we need to keep an eye on that, make sure we can stay ahead of it all, and always try to guess how others can be using cyber, which while very challenging, is important. ■

"Unlike many of the ways we've done traditional arms control in the past, **this is an area where we really do have to be working with industry,** because so much is happening outside government and in academia, where they're doing a lot of exploration on emerging technologies."

The Proliferation of Cyber Mercenaries Calls for New Definitions and Updated Laws

A Q&A with PETER MICEK

General Counsel and U.N. Policy Manager at Access Now

Speaking to FP Analytics, Peter Micek of Access Now addressed the ways in which cyber mercenaries are playing a role in hybrid warfare. The following transcript has been edited for clarity and length.

FP Analytics (FPA): What makes a "cyber mercenary," and how are private organizations classified as such, especially under international law?
Peter Micek (PM): It's someone who directly takes part in hostilities, who's specifically recruited to do so, who's motivated by private gain and is not a national or resident of the state parties involved in the conflict nor a member of the armed forces. In light of new technologies, the international community needs to look at this definition and see whether it's fit for the digital age.

FPA: Why are multistakeholder initiatives such as the Cybersecurity Tech Accord and the Global Commission on the Stability of Cyberspace (GCSC) important for preventing and deterring cyber mercenaries?
PM: Access Now is glad to see and take part in these multistakeholder policymaking initiatives that feature deliberations by states, companies, civil society, academics, technologists, and affected communities. We believe that's the best way to make policy in the digital age. Regarding the GCSC, we were excited by their work and that they centered the rights of the public to a safe, secure, stable, and open cyberspace where human rights can flourish.

FPA: How can existing international laws and frameworks be updated or adapted to the digital age?
PM: We need binding international principles that explicitly regulate cyber mercenaries and outline the legal responsibilities of private tech companies and the states that procure and use their tools and services in ways that violate international human rights. There are jurisdictional hurdles to accountability. These companies are often able to change their names, change their domiciles, change their ownership, find private-equity financing, and evade any attempts at pinning them down. For this reason, we support calls by the U.N. High Commissioner for Human Rights for binding rules on the targeted surveillance trade.

FPA: Can you explain the concept of "derivative sovereign immunity" and how cyber mercenaries have used it to avoid liability?
PM: Sovereign immunity means you can't sue a foreign government. In this new space, we have private-sector actors who are selling to governments extremely sophisticated and secret technologies without going through proper procurement processes and procedures. In these cases, those private companies are trying to protect their ability to do business at will. In response to lawsuits in the United States, NSO Group—a company based in Israel that develops the notorious Pegasus spyware product—put up this claim of so-called "derivative sovereign immunity," claiming that private entities are behaving like states, therefore, they deserve the same protections from lawsuits that states enjoy. However, their fight has failed thus far.

FPA: How can states use tools such as sanctions to deter and punish those that use cyber mercenaries?
PM: State sanctions often intend to advance human rights and democratic values and isolate wrongdoers. But these are traditional tools that, without proper attention, may be counterproductive in the digital age, interfering with human rights and humanitarian access. We need to look at ways to better ensure that the authorities and companies responsible for developing and implementing sanctions better understand their human rights impacts in the digital age. There should be ways to levy sanctions against private- and public-sector actors without violating human rights and humanitarian law, without providing further pretexts for censorship, shutdowns, and other measures that arbitrarily restrict access to digital services by communities at risk. And both companies and governments should listen to civil society when told about the potential unintended adverse consequences of certain implementations of sanctions. ■

Technology Will Not Exceed Our Humanity

We must renew our efforts to ensure that justice is not outpaced by the changing character of war.

By KARIM A.A. KHAN KC

Prosecutor of the International Criminal Court

The tools used to commit serious international crimes constantly evolve—from bullets and bombs to social media, the internet, and perhaps now even artificial intelligence. As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another.

International criminal justice can and must adapt to this new landscape. While no provision of the Rome Statute is dedicated to cybercrimes, such conduct may potentially fulfill the elements of many core international crimes as already defined. In particular, the International Committee of the Red Cross has reiterated that cyberattacks must comply with the cardinal principles of distinction and proportionality and should only be directed against military objectives.

There is an emerging consensus among states that cyberspace is not a special domain free from regulation but rather that international law has a clear role to play. I have repeatedly stated that in all situations addressed by the International Criminal Court Office of the Prosecutor, we need to show that the law is able to deliver for those who find themselves on the front lines. And those front lines are no longer just physical: The digital front lines can give rise to damage and suffering comparable to what the founders of the ICC sought to prevent.

Cyber warfare does not play out in the abstract. Rather, it can have a profound impact on people's lives. Attempts to impact critical infrastructure such as medical facilities or control systems for power generation may result in immediate consequences for many, particularly the most vulnerable. Consequently, as part of its investigations, my Office will collect and review evidence of such conduct. We are likewise mindful of the misuse of the internet to amplify hate speech and disinformation, which may facilitate or even directly lead to the occurrence of atrocities.

Cyber operations are sometimes employed as part of a so-called "hybrid" or "gray zone" strategy. Such strategies aim to exploit ambiguity and operate in the area between war and peace, legal and illegal, with the perpetrators often hidden behind proxy actors. This calls for a whole-of-society response, drawing together distinct functions and capabilities to act in a coordinated way. At the international level, the ICC's jurisdiction—clearly defined and complementary to the broader jurisdictions of states—can serve as an important part of that collective response.

"As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another. International criminal justice can and must adapt to this new landscape."

In particular, as the hub of an international justice system in which states, civil society, and international organizations each play their part, the ICC can make several contributions. Through its own proceedings to ensure legal accountability, the ICC may deter offenders. Such proceedings may also help mitigate the ambiguity of hybrid strategies by reinforcing the applicable law and reliably and prominently determining the truth. The Office may also play a supporting or convening role, by not only investigating with a view to prosecutions before the ICC, but also supporting states and other bodies to proceed under their applicable laws.

In all respects, cooperation is key. It is essential for the ICC to build and strengthen partnerships not only with states but also with corporations. This takes commitment on both sides. Microsoft, and in particular its president, has taken a leading role in cooperating with the ICC, supporting international justice and focusing attention on the need for collective action to address areas of global concern. To highlight this emerging trend and explore innovative and cutting-edge responses, this autumn, my Office and Microsoft will jointly convene a cybercrimes-focused event bringing together expert stakeholders across the private and public sectors. This event will feed into the Office's development of a policy paper.

The increasing intensity and frequency of cyber operations also highlight the importance of developing and improving the ICC's own operational practices. This includes ensuring that the ICC is adequately defended against cyber operations. Disinformation, destruction, the alteration of data, and the leaking of confidential information may obstruct the administration of justice at the ICC and, as such, constitute crimes within the ICC's jurisdiction that might be investigated or prosecuted. But prevention remains better than cure.

With the assistance of states, civil society, and technology leaders, the ICC is already actively working to consolidate and upgrade its information systems architecture and technical capabilities. In particular, partnerships with technology leaders such as Microsoft and Planet Labs have helped my Office harness the power of technology on behalf of victims of international crimes and affected communities, including through the enhanced use of artificial and geospatial intelligence to investigate alleged crimes. We can and will go further in these efforts.

Even visionaries such as Albert Einstein are said to have feared that technology might come to exceed our humanity. Undoubtedly, we shall be tested. But through our common efforts—and above all the belief that we can mobilize the law on these new front lines to deliver justice—we may collectively ensure that a more humane world is forged. The ICC will play its part, now and in years to come. ■

Illustration by MATT CHASE

Keeping Civilians Off-Limits in Present and Future Wars

Civilians must be protected from—and should not participate in—military cyber operations.

By DR. CORDULA DROEGE

Chief Legal Officer of the International Committee of the Red Cross

Few principles carry as much weight and consensus as the cardinal principle of distinction in international humanitarian law (IHL). During armed conflicts, the deliberate targeting of civilians and civilian objects is strictly prohibited—be it through conventional weaponry or cyber operations. Every day, the International Committee of the Red Cross communicates with warring parties involved in more than 70 armed conflicts worldwide, reminding them of this absolute obligation. It applies to all armed conflicts, including those in Syria, the Sahel, and Ukraine—the last of which has seen cyber operations on an unprecedented scale and variety.

On the digital front lines, two issues worry us in particular and must be addressed to ensure that civilians are kept off-limits in today's and future wars.

First, unlawful cyber operations targeting civilians. Belligerents are using cyber operations not only against their adversaries but also to target civilians. As a result, new risks arise for populations that are already enduring the horrors of war: Hospital computers in war-ravaged countries no longer serve their purpose, electricity networks switch off, and the servers of humanitarian organizations are no longer available.

Cyberspace is not a lawless space; accountability is important to prevent and prosecute violations of IHL. But protecting civilians needs to start earlier. Upholding the law and translating it to the digital age must start in each country, ensuring robust protection for civilians, their assets, and their data in our digitalized societies.

Second, a growing involvement of civilian actors—individuals, hacker groups, and companies—in digital operations related to armed conflicts. This troubling trend blurs the distinction between military and civilian domains and risks eroding the principle of distinction and exposing civilians to new dangers. What should be done to mitigate these risks?

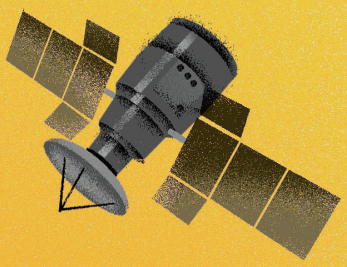
First, states must stop turning a blind eye to private hackers who target civilians. At minimum, states must do what is in their power to ensure that anyone who conducts cyber operations in relation to an armed conflict on their behalf or from their territory respects IHL.

Second, we must beware of the risks that arise when civilians collect battlefield information. Smartphone apps have been developed to encourage civilians to report enemy operations by feeding location-tagged images or videos to the military. While legal experts underline that using apps to collect such information does not automatically make civilians a lawful target, reports suggest that civilians have been shot for being spotted with their smartphones close to military positions. States should refrain from encouraging civilians to participate in hostilities, or at the very least ensure that civilians are aware of the risks and how to protect themselves.

Third, military data and services should not be mixed with civilian ones. The ability and agility of tech companies to respond to cyber operations have been praised, but what unintended consequences arise when they defend infrastructure against military operations or provide cloud storage and communication infrastructure to belligerents? Using civilian infrastructure and services for military purposes exposes them to cyber and kinetic attacks. Concrete measures must be taken to prevent these risks. States should avoid storing military data on nonsegmented civilian clouds and minimize the use of civilian communication infrastructure for military purposes.

What Next? The growing involvement of civilians and the targeting of civilian objects in digital operations expose populations to new harms and risk undermining the universally supported principle of distinction. We must reverse this trend.

Forthcoming recommendations from the ICRC's Global Advisory Board on protecting civilians against digital threats aim to ignite a conversation among governments, companies, and civil society. Together, we must ensure that civilians are shielded from the perils of the digital front lines. ■



Preparing for the Next Hybrid Conflict

Closing thoughts from BRAD SMITH

Vice Chair and President of Microsoft

Thank you for engaging with this special report on cyber operations in armed conflict. While Russia's invasion of Ukraine may be the first example of large-scale hybrid warfare, it will likely not be the last. As cyber operations in warfare evolve, we must work to keep pace by improving cybersecurity and setting and upholding expectations that will limit threats to innocent civilians in this new domain of conflict.

For governments, this means investing in cybersecurity, especially when it comes to protecting critical infrastructure. Having a well-organized and trusted national computer emergency response team (CERT) in Ukraine has been a key differentiator throughout Russia's invasion, enabling rapid response to cyber incidents and coordination with partners across sectors and countries. Migrating critical data to the cloud has also proved an effective cybersecurity measure. These should be priorities for all governments thinking about national security and defense.

The technology industry also has responsibilities when it comes to cyber operations in armed conflict. Without ever engaging in offensive activity itself, the tech sector can and should work to deter cyber operations in three ways: 1) by hardening defenses through improved cybersecurity of our products, 2) by working directly with CERTs and other authorities to protect against cyberattacks, and 3) by sharing information on cyber incidents.

> "I am especially optimistic about the potential for industry to now leverage artificial intelligence as a game-changing technology for security."

I am especially optimistic about the potential for industry to now leverage artificial intelligence as a game-changing technology for security, to autonomously detect and mitigate malicious activity and thereby reduce the impact of cyber operations. Given the resources required to develop and operationalize this next generation of AI, this should give an asymmetric advantage to defenders moving forward.

Improving defenses is only half the equation; we also need more accountability for actors engaging in reckless cyber operations. International humanitarian law (IHL) prohibits attacks on noncombatants and critical civilian infrastructure. Things like kinetic attacks on hospitals, for instance, would be considered war crimes. We cannot afford to allow ambiguities to creep in when it comes to applications of IHL to the online environment. It is therefore encouraging to see the International Criminal Court paying close attention to this issue and weighing whether charges are warranted based on cyber operations in Ukraine.

I want to thank the contributors to this report and our partners at FP Analytics for providing such a comprehensive analysis of these issues and bringing this timely discussion to the fore. While there remain important questions, we must learn from these events to ensure that in future armed conflicts clear guardrails are set around the use of cyber operations. Microsoft looks forward to continued cooperation with partners across stakeholder groups to protect and defend the peaceful use of technology. ■

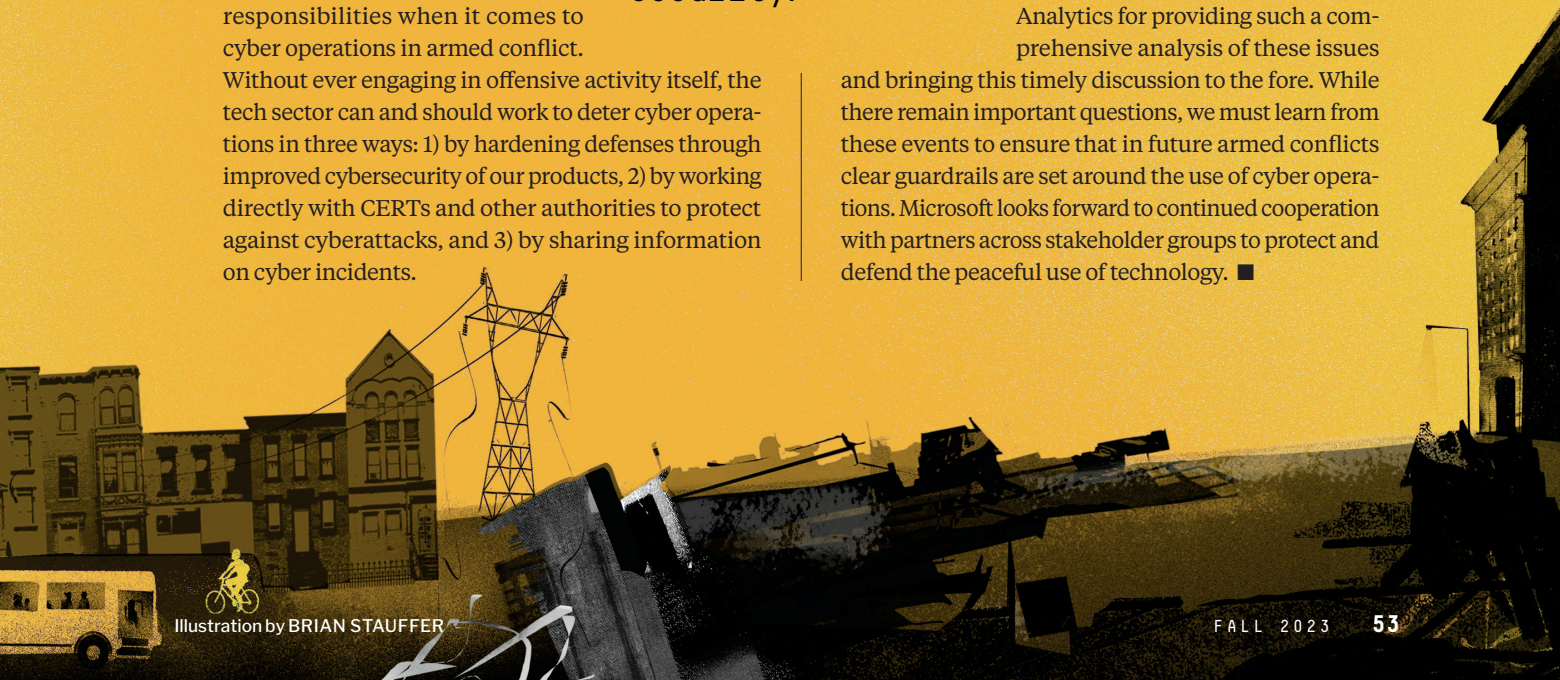


Illustration by BRIAN STAUFFER

BIBLIOGRAPHY

Acronis. (2020, Feb. 7). *The NHS cyber attack.*

Adam, L. (2023, April 20). *In Ukraine, 'wiper' malware is used as a weapon of war.* Le Monde.

Aly, H. (2022, June 2). *Is Ukraine a game-changer for aid and the private sector?* The New Humanitarian.

Amnesty International. (2022, March 9). *Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence.*

Antoniuk, D. (2023, Jan. 20). *Ukraine signs agreement to join NATO cyber defense center.* The Record.

Atlantic Council's Gray Zone Task Force. (2022, Dec. 22). *Scoping the gray zone: Defining terms and policy priorities for engaging competitors below the threshold of conflict.* Atlantic Council.

Bachman, J. (2022, April 6). *U.S. Sends 5,000 SpaceX Starlink Internet Terminals to Ukraine.* Bloomberg.

Bandura, R., Mendez Leal, E.I. (2022, July 18). *The Digital Literacy Imperative.* CSIS.

Banks, W. (2022, Aug. 8). *Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation.* Georgetown Journal of International Affairs.

Basu, A., Poetranto, I., Lau, J. (2021, May 19). *The UN Struggles to Make Progress on Securing Cyberspace.* Carnegie Endowment for International Peace.

Bateman, J. (2022, Dec. 16). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.* Carnegie Endowment for International Peace.

Baugh, S. (2022, March 24). *Responding to Russia's Invasion.* Government Communication Service.

BBC News. (2017, Dec. 19). *Cyber-attack: US and UK blame North Korea for WannaCry.*

Beatty, T., The Associated Press. (2023, Feb. 23). *Microsoft tops the list of largest private donors to Ukraine with $430 million – but Google also made the cut.* Fortune.

Beecroft, N. (2022, Nov. 3). *Evaluating the International Support to Ukrainian Cyber Defense.* Carnegie Endowment for International Peace.

Bellingcat. (n.d.). *Civilian Harm in Ukraine.* Retrieved 07/17/23.

Bennett, V. (2022, Dec. 16). *EBRD helps Ukraine postal operator provide internet, charging points.* European Bank of Reconstruction and Development.

Biden White House. (2023, July 13). *Fact Sheet: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan.*

Black, D. (2023, March 28). *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences.* IISS.

Bogdanova, I. (2022, Sept. 26). *The Role of Technology Sanctions in Crippling Russia's War Machine.* IISD.

Bremmer, I. (2023, July 17). *The Next Global Superpower Isn't Who You Think.* Foreign Policy.

Brilingaite, A., Bukauskas, L., Juozapavicius, A., Kutka, E. (2022, Jan. 28). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity, 8*(1).

Brumfield, C. (2022, June 21). *Space-based assets aren't immune to cyberattacks.* CSO.

Bureau of Arms Control, Verification, and Compliance. (2023, Feb. 16). *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.* U.S. Department of State.

Burgess, M. (2022, March 23). *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine.* Wired.

Business & Human Rights Resource Centre. (2021, Sept. 27). *Investigation finds NSO Group spyware sold to governments used against activists, politicians & journalists; company denies allegations.*

Carter, R.A., Enoizi, J. (2021, March). *Mapping a Path to Cyber Attribution Consensus.* The Geneva Association.

CCDCOE. (2022). *Ukraine to be accepted as a Contributing Participant to NATO CCDCOE.*

CCDCOE. (n.d.). *A surprising turn of events: UN creates two working groups on cyberspace.*

CCDCOE. (n.d.). *About Us.*

CCDCOE. (n.d.). *Power grid cyberattack in Ukraine (2015).* Retrieved 07/14/23.

CCDCOE. (n.d.). *Scenario 18: Legal status of cyber operators during armed conflict.* Retrieved 07/14/23.

CCDCOE. (n.d.). *The Tallinn Manual: Contribute to the Tallinn Manual.*

CEE Multi-Country News Center. (2023, Jan. 20). *How technology helped Ukraine resist during wartime.* Microsoft.

CIMA. (n.d.). *Center for International Media Assistance.* National Endowment for Democracy.

Collier, K. (2022, March 1). *Apple halts sales of products to Russia, restricts access to Russian news apps.* NBC News.

Collier, R. (2017, June 5). NHS Ransomware attack spreads worldwide. *Canadian Medical Association Journal, 189(22):* E786–E787.

Conger, K. (2022, April 12). *Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid.* The New York Times.

Connell, M., Vogler, S. (2016, Sept.). *Russia's Approach to Cyber Warfare.* CNA.

Cordell, C. (2017, Oct. 20). *Tony Scott calls IT workforce drain a 'creeping' crisis bigger than Y2K.* FedScoop.

Corn, G. (2023, Jan. 06). *Cyber Conflict: From Apathy to Action.* American Bar Association.

Council of the EU. (2022, Feb. 25). *Russia's military aggression against Ukraine: EU imposes sanctions against President Putin and Foreign Minister Lavrov and adopts wide ranging individual and economic sanctions.* European Council.

Council of the EU. (2022, March 2). *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU.* European Council.

Council of the EU. (2022, Oct. 6). *EU adopts its latest package of sanctions against Russia over the illegal annexation of Ukraine's Donetsk, Luhansk, Zaporizhzhia and Kherson regions.* European Council.

Council of the EU. (2023, Feb. 25). *One year of Russia's full-scale invasion and war of aggression against Ukraine, EU adopts its 10th package of economic and individual sanctions.* European Council.

Council of the EU. (2022, May 10). *Russian cyber operations against Ukraine Declaration by the High Representative on behalf of the European Union.* European Council.

Council on Foreign Relations. (n.d.). *NotPetya.*

Council on Foreign Relations. (n.d.). *Stuxnet.*

Crowdstrike. (2023, Feb. 28). *Threat Actor.*

Cyber Tech Accord. (n.d.). About the Cybersecurity Tech Accord.

CyberPeace Institute. (2022, June). *Case Study: Viasat.*

CyberPeace Institute. (n.d.). *Cyber Attacks in Times of Conflict: Platform #Ukraine.*

CyberPeace Institute. (n.d.). *CyberPeace Institute.*

Dassa Kaye, D. (2023, Feb. 27). *Israel's Dangerous Shadow War with Iran: Why the Risk of Escalation is Growing.* Foreign Affairs.

Dassault Systems. (2022, March 09). *Dassault Systems Suspends Business Operations in Russia.*

Delerue, F. (2020, Feb. 28). The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack. In F. Delerue (ed.). *Cyber Operations and International Law.* Cambridge University Press.

Digital Security Unit. (2022, April 27). *An overview of Russia's cyberattack activity in Ukraine.* Microsoft.

Dykstra, J., Inglis, C., Walcott, T.S. (2020). Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat. *Joint Force Quarterly, 99(4):* 116–23.

Energy & Commerce Committee. (2023, March 23). *Full Committee Hearing: 'TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms."* 118 Cong.

ESET. (n.d.). *UA Crisis – ESET Response Center.* Retrieved 07/17/23.

Euronews. (2022, Jan 16). *Russia behind website-defacing cyberattack, Ukrainian officials claim.*

European Space Agency. (n.d.). *Cybersecurity.*

Fedorov, M. (2023). *Lessons from Ukraine in the Heat of an Ongoing Hybrid War.* FP Analytics.

Feldstein, S., Kot, B. (2023, March 14). *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.* Carnegie Endowment for International Peace.

Fella, S. (2022, March 22). *The EU response to the Russian invasion of Ukraine.* House of Commons Library.

Foreign, Commonwealth & Development Office. (2022, Nov. 1). *UK boosts Ukraine's cyber defences with £6 million support package.* UK Government.

Fortinet. (n.d.). *What Is Cyberwarfare?*

Fowler, B. (2022, Feb 17). *As Russia's Cyberattacks on Ukraine Mount, the Risk of Impact in Other Countries Rises.* CNET.

FP Analytics. (2023, July 11). *Strategies for Reconciling International Humanitarian Law and Cyber Operations: A Q&A with Dr. Peter Maurer.*

Freeman, L. (2023, April 19). *The Gravity of Russia's Cyberwar against Ukraine.* Opinio Juris.

Gallagher, R. (2023, April 20). *Cyberwar Descends on an Unprepared Moldova.* Bloomberg.

GAO. (2021, April 22). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic).* U.S. Government.

Giannopoulos, G., Smith, H., Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A Conceptual Model.* Hybrid CoE.

Government of Canada. (n.d.). *G7 Rapid Response Mechanism.*

Greenberg, A. (2018, Aug. 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Wired.

Greenberg, A. (2022, May 12). *The Case for War Crimes Charges Against Russia's Sandworm Hackers.* Wired.

Grossi, R. M. (2020, Dec. 10). *Human Rights Day: How Nuclear Science Helps Countries Guarantee Basic Rights to Water, Food and Health.* IAEA.

Harding, E., Ghoorhoo, H. (2023, April). *Seven Critical Technologies for Winning the Next War.* CSIS.

Hern, A. (2022, Oct. 14). *Elon Musk's SpaceX says it can no longer fund Starlink internet in Ukraine.* The Guardian.

Hocking, B., Melissen, J. (2015, July). *Diplomacy in the Digital Age.* Clingendael.

Huang, Z., Ying, Y. (2021, March). *The application of the principle of distinction in the cyber context: A Chinese perspective.* International Review.

Human Rights Center. (n.d.). *Berkley Protocol on Digital Open Source Investigations.* UC Berkley.

Husch, P., Jarnecki, J. (2023, June 1). *All Quiet on the Cyber Front? Explaining Russia's Limited Cyber Effects.* RUSI.

Hybrid CoE. (n.d.). *Hybrid Threats.* Hybrid CoE.

ICRC. (2014, Jan. 1). *The Geneva Conventions of 1949 and their Additional Protocols.*

Igrutinovic, S. (2022, Dec. 16). *EBRD enhances cybersecurity awareness in Moldova.* European Bank of Reconstruction and Development.

Industrie Digitalisierung. (2022, March 7). *Autodesk immediately ceases business in Russia.*

Industrie Digitalisierung. (2022, May 7). *PTC Ceases Business in Russia.*

Insikt Group. (2023, Feb. 9). *Themes and Failures of Russia's War Against Ukraine.* Recorded Future.

Interfax. (2022, July 7). *Oracle gets Ukraine Peace Prize.*

International Atomic Energy Agency. (n.d.). *International Atomic Energy Agency.*

Into the Grey Zone. (2021, Feb. 7). *Episode Five: Cyber Power (Part III) – Hacking ISIS.* Sky News.

ISC2. (2022). *Cybersecurity Workforce Study.*

Iyengar, R. (2023, July 24). *Washington Tries to Add Some Teeth to Its Cyberdefenses.* Foreign Policy.

Jensen, E.T. (2018). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law Vol. 48*: 735–78.

Jones, M.O. (2020, Jan. 20). *Saudi Arabia's bot army flourishes as Twitter fails to tame the beast.* Middle East Eye.

Jordan, E. (2022, March 4). *Gers: une panne de réseau causée par une cyberattaque touche des clients de NordNet.* La Depeche.

Kagubare, I. (2022, March 13). *US, EU cyber investments in Ukraine pay off amid war.* The Hill.

Kallas, K. (2023, April 17). *Kaja Kallas says Ukraine is giving the free world a masterclass on cyber-defence.* The Economist.

Kelley, M.B. (2013, Nov. 20). *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought.* Insider.

Koepke, P. (2017, June). *Cybersecurity Information Sharing Incentives and Barriers.* MIT Management Sloan School.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., Oberholtzer, J. (2017). *Lessons from Russia's Operations in Crimea and Eastern Ukraine.* Rand Corporation.

Kottasova, I. (2023, February). *Russia's war on Ukraine, one year on.* CNN.

LAC4. (n.d.). *Vision.* https://www.lac4.eu/vision/

Lee, R.M., Assante, M.J., Conway, T. (2016, March 18). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Electricity Information Sharing and Analysis Center.

Leonard, B. (2023, April 19). *Ukraine remains Russia's biggest cyber focus in 2023.* Google Threat Analysis Group.

Levite, A., Lee, J. (2022, March 28). *Attribution and Characterization of Cyber Attacks.* Carnegie Endowment for International Peace.

Lucas, R. (2020, Aug. 18). *Senate Releases Final Report on Russia's Interference In 2016 Election.* NPR.

Macias, A., Sheetz, M. (2023, June 01). *Pentagon awards SpaceX with Ukraine contract for Starlink satellite internet.* CNBC.

Mackinnon, A., Iyengar, R. (2022, Dec. 16). *Whatever Happened to Russia's Vaunted Cyberoffensive?* Foreign Policy.

Madnick, S. (2022, March 7). *What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare.* Harvard Business Review.

Maitland, E., Roache, M., Tewa, S. (2023, Feb.). *Misinformation Monitor: February 2023.* NewsGuard.

Mandiant. (n.d.). *Ukraine Crisis Resource Center.*

Manson, K. (2022, March 30). *Cyber War Talks Heat Up at UN With Russia at Table.* Bloomberg.

Mansoor, P.R. (2012, July). Hybrid Warfare in History. In W. Murray and P. R. Mansoor (Eds.), *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present.* (pp. 1–18). Cambridge University Press.

Marin, A. (2023, July 12). *NATO allies' new cyber pledges to remain classified – but here's what we know.* The Record.

Marquardt, A. (2022, Oct. 14). *Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab.* CNN.

Maschmeyer, L. (2021, Oct. 25). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security, 46(2)*: 51–90.

Mazzetti, M., Goldman, A., Bergman, R., Perlroth, N. (2019, March 21). *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments.* The New York Times.

McCurdy, W. (2022, July 07). *Microsoft and AWS awarded Ukrainian peace prize for cloud efforts.* TechRadar.

Microsoft Threat Intelligence. (2023, July 14). *Analysis of Storm-0558 techniques for unauthorized email access.* Microsoft.

Microsoft Threat Intelligence. (2023, March 15). *A year of Russian hybrid warfare in Ukraine.*

Microsoft Threat Intelligence. (2023, May 2). *Iran turning to cyber-enabled influence operations for greater effects.*

Microsoft. (2022, June 22). *Defending Ukraine: Early Lessons from the Cyber War.*

Quiz answers: 1. C; 2. D; 3. B; 4. A; 5. A; 6. B; 7. D; 8. A; 9. D; 10. D

Use the QR code to access the full version of the **Digital Front Lines** report online.

or visit

DigitalFrontLines.io

You'll find additional infographics, extended transcripts of Q&A's, and contributions from **Hanno Pevkur** (Minister of Defense of Estonia) and **Sorin Ducaru** (Director of the EU Satellite Centre).

BIBLIOGRAPHY

Microsoft. (2022). *Microsoft Digital Defense Report 2022: Illuminating the threat landscape and empowering a digital defense.*

Microsoft. (n.d.). *Threat Intelligence.*

Miller, M. (2022, Aug. 2). *Taiwan presidential office website hit by cyberattack ahead of Pelosi visit.* Politico.

Miller, M. (2022, Sept. 7). *Ukraine's largest telecom stands against Russian cyberattacks.* Politico.

Nadelnyuk, O. (n.d.). *How Russian 'Troll factory' tried to effect on Ukraine's agenda. Analysis of 755,000 tweets.* Vox Ukraine.

Nakashima, E., Warrick, J. (2012, June 2). *Stuxnet was work of U.S. and Israeli experts, officials say.* The Washington Post.

Namestnik, V. (2023, Jan. 20). *How Russian Propaganda Constructs an Alternative Reality in Eastern Europe.* Detector Media.

National Academy of Public Administration. (n.d.). *A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Future.* Retrieved 07/31/23.

National Cyber Security Centre. (2023, April 20). *New analysis highlights strength of Ukraine's defence against "unprecedented" Russian offensive.* UK Government.

National Cyber Security Centre. (2022, Feb. 18). *UK government asses Russian involvement in DDoS attacks on Ukraine.* UK Government.

NATO StratCom. (2015). *Analysis of Russia's Information Campaign Against Ukraine.* NATO.

NATO. (2022, June 30). *NATO 2022 Strategic Concept.*

NATO. (2023, July 11). *Vilnius Summit Communiqué.*

NATO. (2023, June 22). *Emerging and disruptive technologies.*

Nuclear Threat Initiative. (n.d.). *Addressing Cyber-Nuclear Security Threats.*

OECD. (2022, Nov. 3). *Disinformation and Russia's war of aggression against Ukraine.*

OECD. (2023, March 21). *Building a Skilled Cyber Security Workforce in Five Countries.*

Oladimeji, S., Kerner, S.M. (2022, June 29). *SolarWinds hack explained: Everything you need to know.* TechTarget.

Orden, H., Pamment, J. (2021, Jan. 26). *What Is So Foreign About Foreign Influence Operations?* Carnegie Endowment for International Peace.

Orenstein, M. (2022, June 7). *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War.* Foreign Policy Research Institute.

OSCE. (2016, March 10). *Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.*

Ottis, R. (2018). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Cooperative Cyber Defence Centre of Excellence.

Park, D., Walstrom, M. (2017, Oct. 11). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.* JSIS.

Pearson, J. (2022, April 12). *Ukraine says it thwarted Russian cyberattack on electricity grid.* Reuters.

Pearson, J., Landay, J. (2022, Feb. 28). *Cyberattack on NATO could trigger collective defence clause – official.* Reuters.

Portnov, A. (2016, June 22). *Bandera mythologies and their traps for Ukraine.* openDemocracy.

Powell, O. (2023, Jan. 5). *IOTW: Almost 50,000 UK government workers vulnerable to cyberattacks.* CyberSecurity Hub.

Prince, M. (2022, March 7). *Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia.* Cloudflare.

Przetacznik, J., Tarpova, S. (2022, June). *Russia's war on Ukraine: Timeline of cyber-attacks.* European Parliamentary Research Service.

Rattray, G., Brown, G., Moore, R. T. (2023, February). *The Cyber Defense Assistance Imperative: Lessons from Ukraine.* Aspen Institute.

Roache, M., et al. (2023, July 10). *Russia-Ukraine Disinformation Tracking Center: 382 Websites Spreading War Disinformation and the Top Myths they Publish.* NewsGuard. Retrieved 07/14/23.

Sabbagh, D. (2023, Feb. 9). *Fury in Ukraine as Elon Musk's SpaceX limits use for drone.* The Guardian.

Saunders, B., Cooper, A. (2023, January). *Advancing Cyber Norms Unilaterally: How the U.S. Can Meet its Paris Call Commitments.* Belfer Center for Science and International Affairs.

Seldin, J. (2023, Feb. 27). *US Warns of Massive Chinese Cyberattacks in Taiwan Scenario.* VoA.

Sheahan, M., Steitz, C., Rinke, A. (2022, Feb. 28). *Satellite outage knocks out thousands of Enercon's wind turbines.* Reuters.

Silverman, C., Kao, J. (2022, March 11). *Infamous Russian Troll Farm Appears to be Source of Anti-Ukraine Propaganda.* ProPublica.

Singer, P.W., Johnson, E.B., (2021, Feb. 1). *The need to inoculate military servicemembers against information threats: the case for digital literacy training for the force.* War on the Rocks.

Smith, K.V. (2022, May 20). *How Companies Are Responding to the War in Ukraine: A Roundup.* Boston College Center for Corporate Citizenship.

Spravdi. (n.d.). *Centre for strategic communication.* Government of Ukraine.

Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities. 116 Cong. (2020, March 4).

Steer, C. (2020, Oct. 26). Why Outer Space Matters for National and International Security. *ANU College of Law Research Paper No. 20.25.*

Stoutland, P.O., Pitts-Kiefer, S. (2018). *Understanding the Cyber Threat to Nuclear Weapons and Related Systems.* Nuclear Threat Initiative.

Strobel, W.P. (2022, Dec. 22). *U.S. Has Eased Intelligence-Sharing Rules to Help Ukraine Target Russians.* The Wall Street Journal.

Swinhoe, D. (2019, May 30). *Why businesses don't report cybercrimes to law enforcement.* CSO.

Tangalakis-Lippert, K. (2022, Dec. 18). *Amazon helped rescue the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: 'You can't take out the cloud with a cruise missile'.* Insider.

The Stack. (2022, Nov. 30). *How Ukrainian, AWS officials scrambled to save government data.*

Trump White House. (2017, Dec. 19). *Press Briefing on the Attribution of WannaCry Malware Attack to North Korea.* The White House.

U.S. Department of State. (2022, May 10). *U.S. Support for Connectivity and Cybersecurity in Ukraine.*

U.S. Department of State. (2023, April). *Guiding Principles on Government Use of Surveillance Technologies.*

U.S. Department of State. (2023, June 5). *Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue.*

U.S. Department of the Treasury. (2022, March 31). *Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War.*

Ukraine Conflict Observatory. (n.d.). *About Us.*

UkraineFacts. (n.d.).

UkraineNow. (n.d.). *Secure Critical Infrastructure of Ukraine.*

UN General Assembly. (2021, July 13). *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266.* United Nations.

UN General Assembly. (2021, March 10). *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report.* United Nations.

UN IGF. (2022). *IGF 2022 WS #361 Navigating the age of hybrid warfare.* United Nations.

UN Office for Disarmament Affairs. (2021). *Open-ended Working Group on security of and in the use of information and communications technologies.* United Nations.

UN Secretary General. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General.* United Nations Digital Library.

UNDP Ukraine. (n.d.). *Call for participation in competition 'Countering fake news, disinformation and propaganda in Ukraine."* UNDP.

United Nations Meetings Coverage and Press Releases. (2014, March 27). *General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region.*

United Nations. (2023, July). *Our Common Agenda Policy Brief 9: A New Agenda for Peace.*

Verbyany, V., Krasnolutska, D. (2022, Dec. 20). *Ukraine to Get Thousands More Starlink Antennas, Minister Says.* Bloomberg.

Vest, N., Clarke, C.P. (2020, June 2). *Is the Conflict in Libya a Preview of the Future of Warfare?* Defense One.

Virgo, P. (2023, May 23). *Making sense of the UK Cybersecurity Skills market.* Computer Weekly.

Vox Ukraine. (n.d.). VoxCheck.

Wakefield, J. (2022, March 18). *Deepfake presidents used in Russia-Ukraine war.* BBC News.

Walker, K. (2022, Dec. 1). *New ways we're supporting Ukraine.* Google The Keyword.

Warren, T. (2022, June 8). *Microsoft winds down its business in Russia, lays off more than 400 people.* The Verge.

Watts, C. (2023, May 2). *Rinse and repeat: Iran accelerates its cyber influence operations worldwide.* Microsoft.

Watts, C. (2022, Dec. 3). *Preparing for a Russian cyber offensive against Ukraine this winter.* Microsoft.

Wiessmann, M., Nilsson, N., Thunholm, P., Palmertz, B. (eds.). (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations.*

Wolff, J. (2021, Dec. 1). *How the NotPetya attack is reshaping cyber insurance.* Brookings Institution.

Wong, E., Jakes, L. (2022, Jan. 13). *NATO Won't Let Ukraine Join Soon. Here's Why.* The New York Times.

World Economic Forum. (2023). *The Global Risks Report 2023.*

Wu, S., Baptista, E. (2022, Aug. 4). *From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit.* Reuters.

Young, B.R. (2022, Feb. 9). *North Korea Knows How Important Its Cyberattacks Are.* Foreign Policy.

Zetter, K. (2022, Sept. 26). *Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Officials Say.* Zetter.

QUIZ

Answers on page 55

PART ONE

1. From July 2020 to July 2021, 19 percent of the global nation-state threat activity warnings that Microsoft issued were made to customers in which country, second only to the United States?

a. Belgium
b. Germany
c. Ukraine
d. Israel

2. Which of the following is NOT a member of the intelligence alliance the Five Eyes?

a. United States
b. United Kingdom
c. Canada
d. Netherlands

3. The first and most notable act of cyber attribution was when the cybersecurity firm Mandiant in 2013 released the APT1 report, which exposed a large-scale cyber campaign by which country's military?

a. Russia
b. China
c. Iran
d. North Korea

4. Before Russia's invasion, the Ukrainian government's Red Team prepared for cyber operations by:

a. Crash-testing state information systems around the clock to find vulnerabilities
b. Holding global competitions for hackers to identify cybersecurity gaps
c. Transferring government and private-sector data to cloud platforms
d. Training the next generation of military and civilian cyber professionals

PART TWO

5. What is the concept of deterrence by denial?

a. Dissuading an adversary from attacking by convincing it that an attack will not achieve its intended goal
b. Dissuading an adversary from attacking using strong negative diplomatic statements
c. Dissuading an adversary from attacking by attacking pre-emptively
d. Dissuading an adversary from attacking by joining a diplomatic treaty with them

6. What kind of technology is NSO Group's Pegasus software?

a. Wiper
b. Spyware
c. Ransomware
d. Bot

7. Who hosts the world's largest international cyber defense exercises?

a. The African Union's Peace and Security Council
b. Russia's Main Directorate of the General Staff of the Armed Forces
c. The European Union Naval Force
d. NATO's Cooperative Cyber Defence Centre of Excellence

PART THREE

8. Cuba, Nicaragua, and _____ have the highest levels of Russian propaganda consumption in Latin America.

a. Venezuela
b. Dominican Republic
c. Puerto Rico
d. Brazil

9. Which of the following is not within the mandate of the International Criminal Court Office of the Prosecutor?

a. Investigating with a view to prosecute before the ICC
b. Supporting states and other bodies to proceed with prosecutions under their applicable laws
c. Playing a convening role within the international legal community
d. Operating a prison for international cyber criminals

10. Which of the following is not an example of blurred lines between civilian and military domains?

a. Storing military data on nonsegmented civilian clouds
b. Civilians collecting battlefield information and reporting enemy operations to their military
c. Outer space-based equipment that provides both civilian and military services
d. A missile targeting an enemy tank

“Just as governments rely on air defense systems to repel missiles, they should invest in creating cybersecurity iron domes to repel cyberattacks.”

Mykhailo Fedorov, Vice Prime Minister for Innovations, Development of Education, Science, and Technologies and Minister of Digital Transformation of Ukraine

“As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another. International criminal justice can and must adapt to this new landscape.”

Karim A.A. Khan KC, Prosecutor of the International Criminal Court

“We have to find ways to constantly stay ahead of countries or other entities that want to use cyber in ways that can be even more devastating in terms of weapons of mass destruction.”

Ambassador Bonnie Jenkins, Under Secretary for Arms Control and International Security, U.S. Department of State

“Because of the unique nature of cybersecurity and cyberspace itself, various actors from civil society, industry, the private sector, and academia need to play a role in the advancement of responsible behavior in the cyber domain and the implementation of confidence-building and capacity-building initiatives.”

Izumi Nakamitsu, U.N. Under-Secretary-General and High Representative for Disarmament Affairs