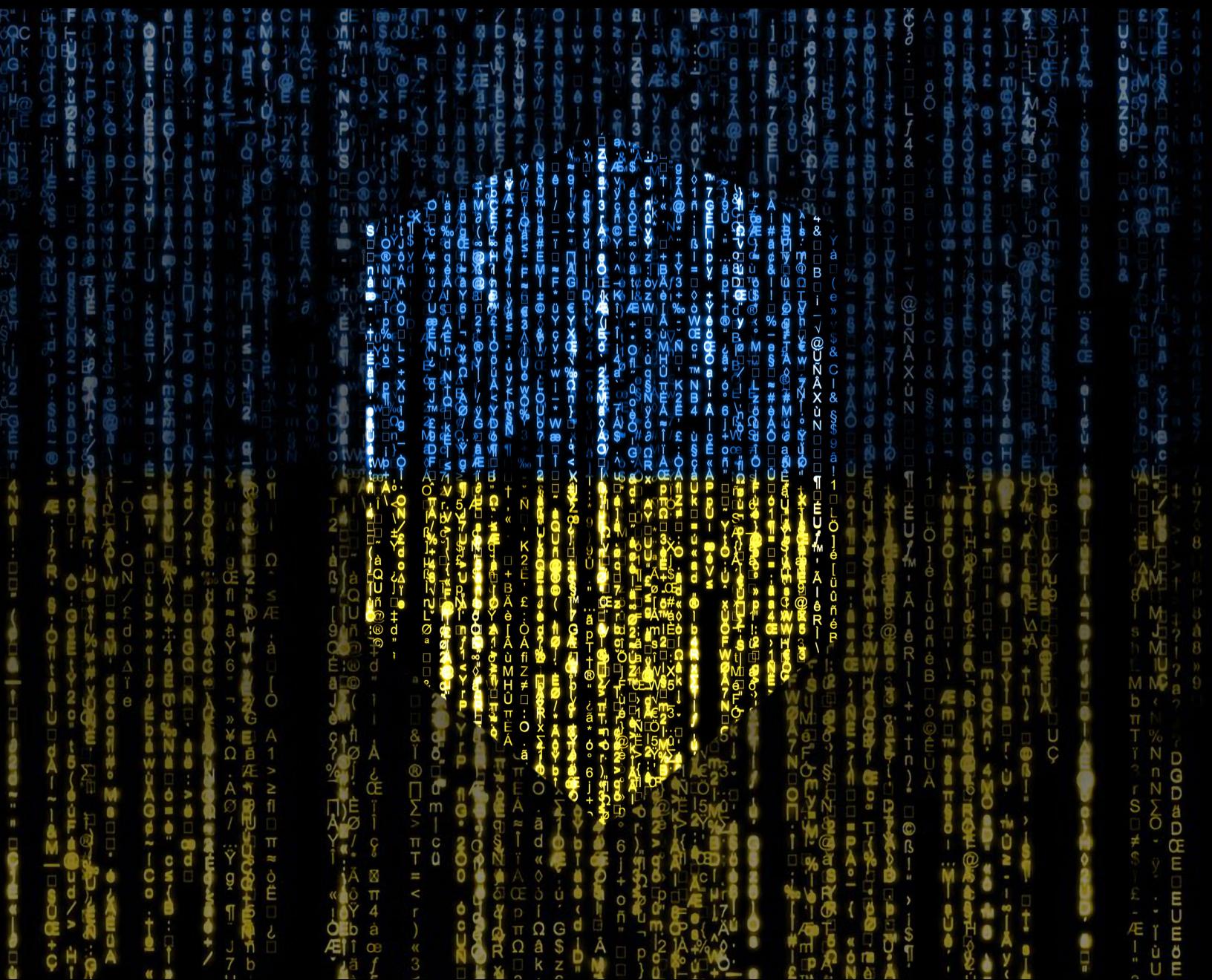




# Defending Ukraine: Early Lessons from the Cyber War



## Foreword



Brad Smith, President  
and Vice Chair, Microsoft

The recorded history of every war typically includes an account of the first shots fired and who witnessed them. Each account provides a glimpse not just into the start of a war, but the nature of the era in which people lived.

Historians who discuss the first shots in America's Civil War in 1861 typically describe guns, cannons, and sailing ships around a fort near Charleston, South Carolina.

Events spiraled toward the launch of World War I in 1914 when terrorists in plain view on a city street in Sarajevo used grenades and a pistol to assassinate the archduke of the Austrian-Hungarian Empire.

It would take until the Nuremberg war trials to fully understand what happened near the Polish border 25 years later. In 1939, Nazi SS troops dressed in Polish uniforms and staged an attack against a German radio station. Adolf Hitler cited such attacks to justify a blitzkrieg invasion that combined tanks, planes, and troops to overrun Polish cities and civilians.

Each of these incidents also provides an account of the technology of the time—technology that would play a role in the war that ensued and the lives of the people who lived through it.

The war in Ukraine follows this pattern. The Russian military poured across the Ukrainian border on February 24, 2022, with a combination of troops, tanks, aircraft, and cruise missiles. But the first shots were in fact fired hours before when the calendar still said February 23. They involved a cyberweapon called "Foxblade" that was launched against computers in Ukraine. Reflecting the technology of our time, those among the first to observe the attack were half a world away, working in the United States in Redmond, Washington.

As much as anything, this captures the importance of stepping back and taking stock of the first several months of the war in Ukraine, which has been devastating for the country in terms of destruction and loss of life, including innocent civilians. While no one can predict how long this war will last, it's already apparent that it reflects a trend witnessed in other major conflicts over the past two centuries. Countries wage wars using the latest technology, and the wars themselves accelerate technological change. It's therefore important to continually assess the impact of the war on the development and use of technology.

The Russian invasion relies in part on a cyber strategy that includes at least three distinct and sometimes coordinated efforts—destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world. This report provides an update and analysis on each of these areas and the coordination among them. It also offers ideas about how to better counter these threats in this war and beyond, with new opportunities for governments and the private sector to work better together.

The cyber aspects of the current war extend far beyond Ukraine and reflect the unique nature of cyberspace. When countries send code into battle, their weapons move at the speed of light. The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls, and oceans. And the internet itself, unlike land, sea, and the air, is a human creation that relies on a combination of public and private-sector ownership, operation, and protection.

This in turn requires a new form of collective defense. This war pits Russia, a major cyber-power, not just against an alliance of countries. The cyber defense of Ukraine relies

critically on a coalition of countries, companies, and NGOs.

The world can now start to assess the early and relative strengths and weaknesses of offensive and defensive cyber operations. Where are collective defenses successfully thwarting attacks and where are they falling short? What types of technological innovations are taking place? And critically, what steps are needed to effectively defend against cyberattacks in the future? Among other things, it's important to base these assessments on accurate data and not be misled into an unwarranted sense of tranquility from the external perception that the cyberwar in Ukraine has not been as destructive as some feared.

**This report offers five conclusions that come from the war's first four months:**

**First, defense against a military invasion now requires for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries.** Russia not surprisingly targeted Ukraine's governmental data center in an early cruise missile attack, and other on-premises servers similarly were vulnerable to attacks by conventional weapons. Russia also targeted its destructive "wiper" attacks at on-premises computer networks. But Ukraine's government has successfully sustained its civil and military operations by acting quickly to disburse its digital infrastructure into the public cloud, where it has been hosted in data centers across Europe.

This has involved urgent and extraordinary steps from across the tech sector, including by Microsoft. While the tech sector's work has been vital, it's also important to think about the longer-lasting lessons that come from these efforts.

**Second, recent advances in cyber threat intelligence and end-point protection have helped Ukraine withstand a high percentage of destructive Russian cyberattacks.** Because cyber activities are invisible to the naked eye, they are more difficult for journalists and even many military analysts to track. Microsoft has seen the Russian military launch multiple waves of destructive cyberattacks against 48 distinct Ukrainian agencies and enterprises. These have sought to penetrate network domains by initially

compromising hundreds of computers and then spreading malware designed to destroy the software and data on thousands of others.

Russian cyber tactics in the war have differed from those deployed in the NotPetya attack against Ukraine in 2017. That attack used "wormable" destructive malware that could jump from one computer domain to another and hence cross borders into other countries. Russia has been careful in 2022 to confine destructive "wiper software" to specific network domains inside Ukraine itself. But the recent and ongoing destructive attacks themselves have been sophisticated and more widespread than many reports recognize. And the Russian army is continuing to adapt these destructive attacks to changing war needs, including by coupling cyberattacks with the use of conventional weapons.

A defining aspect of these destructive attacks so far has been the strength and relative success of cyber defenses. While not perfect and some destructive attacks have been successful, these cyber defenses have proven stronger than offensive cyber capabilities. This reflects two important and recent trends. First, threat intelligence advances, including the use of artificial intelligence, have helped make it possible to detect these attacks more effectively. And second, internet-connected end-point protection has made it possible to distribute protective software code quickly both to cloud services and other connected computing devices to identify and disable this malware. Ongoing wartime innovations and measures with the Ukrainian government have strengthened this protection further. But continued vigilance and innovation will likely be needed to sustain this defensive advantage.

**Third, as a coalition of countries has come together to defend Ukraine, Russian intelligence agencies have stepped up network penetration and espionage activities targeting allied governments outside Ukraine.** At Microsoft we've detected Russian network intrusion efforts on 128 organizations in 42 countries outside Ukraine. While the United States has been Russia's number one target, this activity has also prioritized Poland, where much of the logistical delivery of military and humanitarian assistance

is being coordinated. Russian activities have also targeted Baltic countries, and during the past two months there has been an increase in similar activity targeting computer networks in Denmark, Norway, Finland, Sweden, and Turkey. We have also seen an increase in similar activity targeting the foreign ministries of other NATO countries.

Russian targeting has prioritized governments, especially among NATO members. But the list of targets has also included think tanks, humanitarian organizations, IT companies, and energy and other critical infrastructure suppliers. Since the start of the war, the Russian targeting we've identified has been successful 29 percent of the time. A quarter of these successful intrusions has led to confirmed exfiltration of an organization's data, although as explained in the report, this likely understates the degree of Russian success.

We remain the most concerned about government computers that are running on premises rather than in the cloud. This reflects the current and global state of offensive cyber espionage and defensive cyber protection. As the SolarWinds incident demonstrated 18 months ago, Russia's intelligence agencies have extremely sophisticated capabilities to implant code and operate as an Advanced Persistent Threat (APT) that can obtain and exfiltrate sensitive information from a network on an ongoing basis. There have been substantial advances in defensive protection since that time, but the implementation of these advances remains more uneven in European governments than in the United States. As a result, significant collective defensive weaknesses remain.

**Fourth, in coordination with these other cyber activities, Russian agencies are conducting global cyber influence operations to support their war efforts.** These combine tactics developed by the KGB over several decades with new digital technologies and the internet to give foreign influence operations a broader geographic reach, higher volume, more precise targeting, and greater speed and agility. Unfortunately, with sufficient planning and sophistication, these cyber influence operations are well-positioned to take advantage of the longstanding openness of democratic societies and the public polarization that is

characteristic of current times.

As the war in Ukraine has progressed, Russian agencies are focusing their cyber influence operations on four distinct audiences. They are targeting the Russian population with the goal of sustaining support for the war effort. They are targeting the Ukrainian population with the goal of undermining confidence in the country's willingness and ability to withstand Russian attacks. They are targeting American and European populations with the goal of undermining Western unity and deflecting criticism of Russian military war crimes. And they are starting to target populations in nonaligned countries, potentially in part to sustain their support at the United Nations and in other venues.

Russian cyber influence operations are building on and are connected to tactics developed for other cyber activities. Like the APT teams that work within Russian intelligence services, Advance Persistent Manipulator (APM) teams associated with Russian government agencies act through social media and digital platforms. They are pre-positioning false narratives in ways that are similar to the pre-positioning of malware and other software code. They are then launching broad-based and simultaneous "reporting" of these narratives from government-managed and influenced websites and amplifying their narratives through technology tools designed to exploit social media services. Recent examples include narratives around biolabs in Ukraine and multiple efforts to obfuscate military attacks against Ukrainian civilian targets.

As part of a new initiative at Microsoft, we are using AI, new analytics tools, broader data sets, and a growing staff of experts to track and forecast this cyber threat. Using these new capabilities, we estimate that Russian cyber influence operations successfully increased the spread of Russian propaganda after the war began by 216 percent in Ukraine and 82 percent in the United States.

These ongoing Russian operations build on recent sophisticated efforts to spread false COVID-19 narratives in multiple Western countries. These included state-sponsored cyber influence operations in 2021 that sought

to discourage vaccine adoption through English-language internet reports while simultaneously encouraging vaccine usage through Russian-language sites. During the last six months, similar Russian cyber influence operations sought to help inflame public opposition to COVID-19 policies in New Zealand and Canada.

We will continue to expand Microsoft's work in this field in the weeks and months ahead. This includes both internal growth and through the agreement we announced last week to acquire Miburo Solutions, a leading cyber threat analysis and research company specializing in the detection of and response to foreign cyber influence operations.

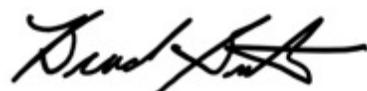
We're concerned that many current Russian cyber influence operations currently go for months without proper detection, analysis, or public reporting. This increasingly impacts a wide range of important institutions in both the public and private sectors. And the longer the war lasts in Ukraine, the more important these operations likely will become for Ukraine itself. This is because a longer war will require sustaining public support from the inevitable challenge of greater fatigue. This should add urgency to the importance of strengthening Western defenses against these types of foreign cyber influence attacks.

**Finally, the lessons from Ukraine call for a coordinated and comprehensive strategy to strengthen defenses against the full range of cyber destructive, espionage, and influence operations.** As the war in Ukraine illustrates, while there are differences among these threats, the Russian government does not pursue them as separate efforts and we should not put them in separate analytical silos. In addition, defensive strategies must consider the coordination of these cyber operations with kinetic military operations, as witnessed in Ukraine.

New advances to thwart these cyber threats are needed, and they will depend on four common tenets and — at least at a high level — a common strategy. The first defensive tenet should recognize that Russian cyber threats are being advanced by a common set of actors inside and outside the Russian government and rely on similar digital tactics. As a result, advances in digital technology, AI, and data will be needed to counter them. Reflecting this, a second tenet should recognize that unlike the traditional threats of the past, cyber responses must rely on greater public and private collaboration. A third tenet should embrace the need for close and common multilateral collaboration among governments to protect open and democratic societies. And a fourth and final defensive tenet should uphold free expression and avoid censorship in democratic societies, even as new steps are needed to address the full range of cyber threats that include cyber influence operations.

An effective response must build on these tenets with four strategic pillars. These should increase collective capabilities to better (1) detect, (2) defend against, (3) disrupt, and (4) deter foreign cyber threats. This approach is already reflected in many collective efforts to address destructive cyberattacks and cyber-based espionage. They also apply to the critical and ongoing work needed to address ransomware attacks. We now need a similar and comprehensive approach with new capabilities and defenses to combat Russian cyber influence operations.

As discussed in this report, the war in Ukraine provides not only lessons but a call to action for effective measures that will be vital to the protection of democracy's future. As a company, we are committed to supporting these efforts, including through ongoing and new investments in technology, data, and partnerships that will support governments, companies, NGOs, and universities.



Brad Smith  
President and Vice Chair

## The Distribution of Digital Operations in Wartime

### 1

The war in Ukraine highlights in part the changes the 21st century has brought to governments around the world. In the Second World War, as bombs fell on London, one key to sustaining the British government was to move its communications equipment underground and into the Cabinet War Rooms. Today, governments rely on digital communications and data, and one key to sustaining the Ukrainian government has been to disburse these digital operations into the public cloud and outside the country itself.

Prior to the war, Ukraine had a longstanding Data Protection Law prohibiting government authorities from processing and storing data in the public cloud. This meant that the country's public-sector digital infrastructure was run locally on servers physically located within the country's borders. A week before the Russian invasion, the Ukrainian government was running entirely on servers located within government buildings—locations that were vulnerable to missile attacks and artillery bombardment.

Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, and his colleagues in Parliament recognized the need to address this vulnerability. On February 17, just days before Russian troops invaded, Ukraine's Parliament took action to amend its data protection law to allow government data to move off existing on-premises servers and into the public cloud. This in effect enabled it to "evacuate" critical government data outside the country and into data centers across Europe.

Several tech companies rallied to help. At Microsoft, we witnessed and supported the speed required for this transition. Within 10 weeks, Ukraine's Ministry of Digital Transformation and more than 90 chief digital

transformation officers across the Ukrainian government worked with the company to transfer to the cloud many of the central government's most important digital operations and data. Microsoft has committed at no charge a total of \$107 million of technology services to support this effort, which has reached 20 ministries and more than 100 state agencies and state-owned enterprises. (In total, Microsoft has provided \$239 million in financial and technology assistance to support Ukraine, including support for the government, businesses, nonprofits, and humanitarian assistance for refugees.)

Fedorov's urgency was prophetic. An early target of Russian missile attacks was a Ukrainian government data center. And as discussed further below, the Russian military has targeted the government's on-premises computer networks with its destructive cyber "wiper" attacks. One reason these kinetic and cyberattacks have had limited operational impact is because digital operations and data have been disbursed into the public cloud.

This highlights a critical difference between protecting public-sector data in a time of war instead of peace. Some governments around the world have pursued initiatives in recent years to centralize government digital operations in so-called sovereign data centers that are more specialized, locally controlled, and located within a country's borders. While there are some factors that make this appealing from a national security perspective in times of peace, the last few months in Ukraine illustrate the very different defense needs that prevail during a war. The key to a country's digital resilience in wartime is the ability quickly to move data outside the country while still connecting to and relying on it for a government's digital operations.

## The Evolution of Offensive Cyberattacks and Defensive Cybersecurity Operations

# 2

Innovation in offensive and defensive military technologies and tactics has been a constant, especially during the past two centuries. Wars put these innovations to new tests. While the “fog of war” makes it more difficult to assess the relative strength of offensive and defensive capabilities, it also creates greater urgency for doing so. The war in Ukraine is no exception, including for cyberattacks and cybersecurity protection.

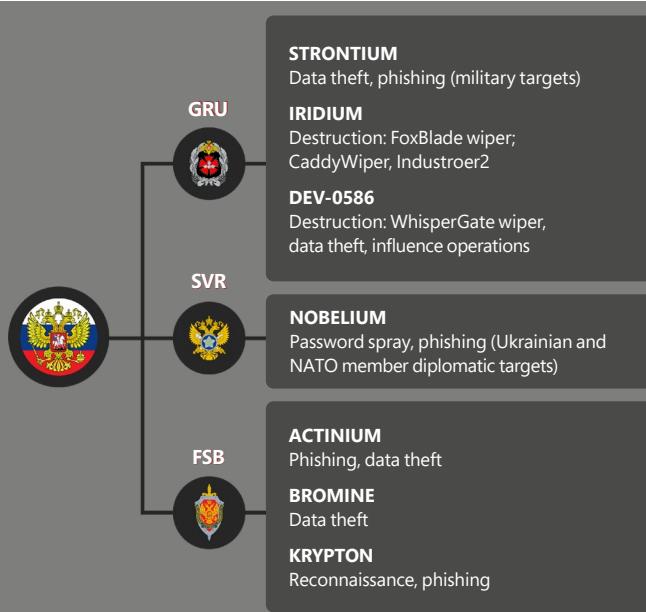
It's perhaps helpful to start with a historical analogy that is well understood. The Battle of Britain in 1940 pitted the use of an offensive technology—the bomber—against the defensive use of two other technologies, more advanced fighters, and the use of radar. The radar waves were invisible to the naked eye, and their widespread use was unknown to the public during the battle itself. But radar was indispensable in enabling the Royal Air Force to detect the oncoming bombers and direct fighters to combat them. While bombers succeeded in dropping bombs on England, they failed strategically in establishing the air supremacy needed to support an invasion.

This history shares some important similarities with the current day. The war in Ukraine has pitted offensive

cyberattacks that are invisible to the naked eye against advances in cybersecurity technologies and operations. Like the bombers of 1940, some of the cyberattacks have succeeded in reaching and disabling their targets. But at a broader level, so far these attacks have failed strategically in disabling Ukraine's defenses. While part of the reason lies in the disbursement of Ukrainian digital operations into the cloud, discussed above, another reason has been the overall ability of cyber defenses to successfully defeat these attacks.

It's important to take note of the destructive cyber tactics the Russian military has deployed in Ukraine. These have three facets. The first aspect, which is also common to ransomware and nation-state cyber espionage, involves targeted phishing and similar efforts to enter a computer network. This tactic reflects the determination, sophistication, and persistence long observed across the cyber activities of Russia's intelligence community and military. The second involves the planting of “wiper” malware designed to “wipe” computer hard disks and destroy all their data. And the third has involved software architecture that is designed to replicate or spread this malware to other computers across a network domain, such as the network of an entire government ministry.

### Russian government entities responsible for cyberattacks



While most reports state that the war in Ukraine started on February 24 of this year, in fact the first cyberattacks were fired the day before. The first weapon to be fired was the wiper software that we call “Foxblade.” Microsoft’s Threat Intelligence Center (MSTIC) has detected its launch against 19 government and critical infrastructure entities across Ukraine. It was developed and launched by the same group associated with Russian military intelligence that developed and launched the NotPetya attack against Ukraine in 2017. (At Microsoft we call this group Iridium, and it’s known by others as Sandworm.)

This initial attack was just the first salvo. Since the war began, MSTIC has detected multiple attempts to use eight distinct malware programs—some wipers and some other forms of destructive malware—against 48 different Ukrainian agencies and enterprises. These have sought, sometimes repeatedly, to penetrate network domains by initially compromising hundreds of computers and then spreading malware to thousands of others. The CyberPeace Institute, an independent and neutral nonprofit headquartered in Geneva and which Microsoft and many others support, similarly has [found a growing number](#) of wiper and other destructive malware attacks.

As the war has progressed, the Russian army has adapted its destructive cyberattacks to its changing war needs. On several occasions the Russian military has coupled its cyberattacks with conventional weapons aimed at the same targets. Like the combination of naval and ground forces long used in an amphibious invasion, the war in Ukraine has witnessed Russian use of cyberattacks to disable computer networks at a target before seeking to overrun it with ground troops or aerial or missile attacks.

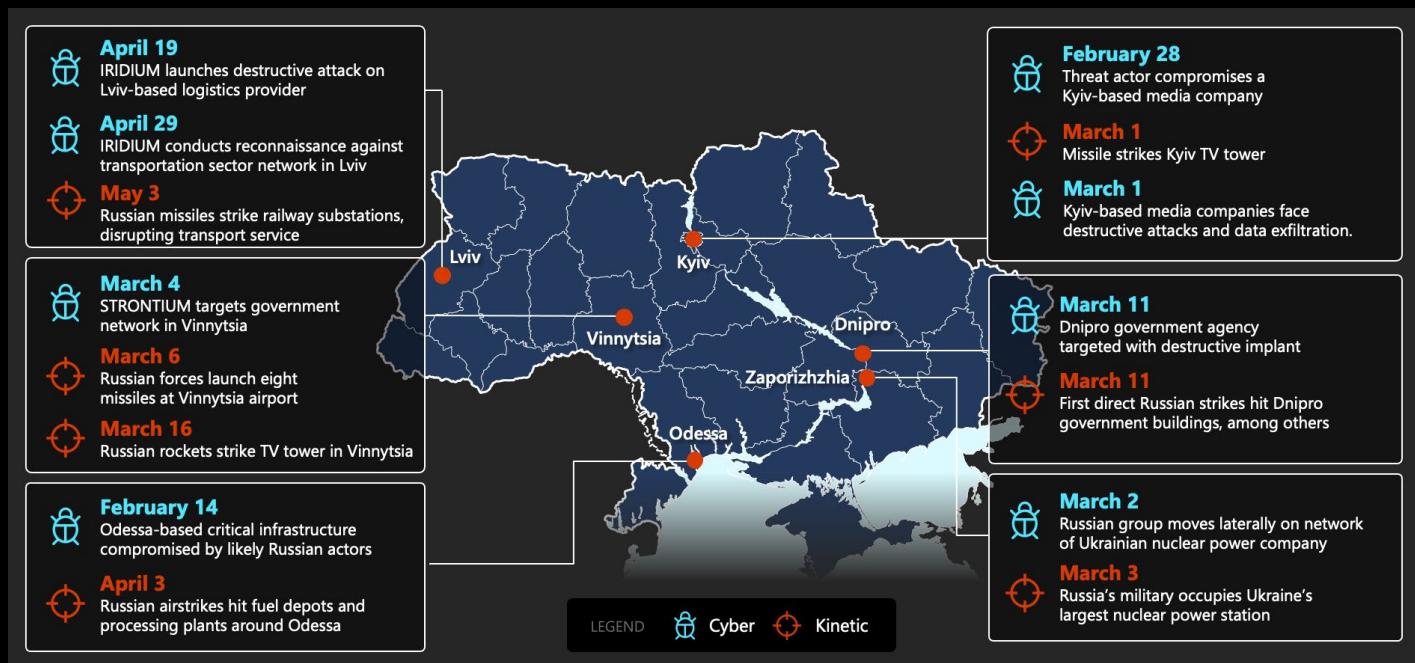
For example, as we listed in the [Special Report on Ukraine](#), published on April 27, the Russian military combined cyber and conventional weapons in assaulting a nuclear power plant in early March. On March 2, MSTIC identified a Russian group moving laterally on the nuclear power company’s computer network. The next day, the Russian military attacked and occupied the company’s largest nuclear power plant. During the same week, the Russian army group MSTIC calls Strontium compromised a government computer network in Vinnytsia and two days later launched eight cruise missiles at the city’s airport. Similarly, on March 11, Russian forces targeted a Dnipro government agency with a destructive cyberattack while also using conventional weapons against government buildings.

### Russian malware families used for destructive attacks

- |                               |                                 |                |                             |
|-------------------------------|---------------------------------|----------------|-----------------------------|
| • WhisperGate / WhisperKill   | • SonicVote, aka HermeticRansom | • DesertBlade  | • Lasainraw, aka IssacWiper |
| • FoxBlade, aka HermeticWiper | • CaddyWiper                    | • Industroyer2 | • FiberLake, aka DoubleZero |

WhisperGate, FoxBlade, DesertBlade, and CaddyWiper are all malware families that overwrite data and render machines unbootable. FiberLake is a .NET capability being used for data deletion. SonicVote is a file encryptor sometimes used together with FoxBlade. Industroyer2 specifically targets operational technology to achieve physical effects in industrial production and processes.

## Coordinated Russian cyber and military operations in Ukraine



It's important to recognize that Russian cyber tactics in the war have been strategic and deliberate but are different from the 2017 NotPetya attack. To date, the Russians haven't used destructive "wormable" malware that can jump from one computer domain to another and thereby cross international borders to spread economic damage. Instead, they are designing attacks to stay within Ukraine. While Russia has been careful to confine its destructive malware to specific network domains located within Ukraine itself, these attacks are more sophisticated and widespread than many reports recognize.

During the past month, as the Russian military moved to concentrate its attacks in the Donbas region, the number of destructive attacks has fallen. More recent destructive cyberattacks have been coordinated with missile attacks and have targeted Ukraine's railways and transportation systems transporting weapons and military supplies. For example, when Russian missiles struck railway substations in Lviv on May 3—a key logistical center for the movement of military and humanitarian aid—the military's Iridium group was already

active within the digital networks of these same agencies.

Since the war began in Ukraine, some observers have expressed surprise at the relative absence of Russian destructive cyberattacks. To some degree, this is based on a comparison to the international destruction wrought by NotPetya, which Russia to date has avoided replicating.

But the more limited impact is attributable to other factors as well. Because cyberattacks are invisible to the naked eye, they tend to be perceived by the public and reported by journalists only when they succeed and computer networks stop operating. And, to date at least, cyber defenses and operations have withstood attacks far more often than they have failed.

Cybersecurity threat intelligence has strengthened in the five years since the NotPetya attack. In the private sector, an organization such as MSTIC now has the benefit of visibility created by 24 trillion signals that Microsoft receives daily from devices and cloud services across a global ecosystem. This enormous global data set is an extraordinary resource that

makes it possible to detect new anomalies more quickly and identify other customers and networks confronting the same attack. Recent advances in AI-based cybersecurity protection are starting to augment this protection even further.

This type of detection capability is especially helpful for organizations using cloud services. For example, in March, Russia's Iridium unit aimed wiper malware at a shipping company in Lviv where the malware was detected on a system running Microsoft Defender with Cloud Protection enabled. An ensemble of AI machine learning models used a combination of signals across the client network and the cloud to block this malware at first sight without any human intervention. While this level of AI-based detection currently cannot be applied outside cloud services, it highlights both the importance of broader recent threat intelligence and analysis and the opportunity for future investments and improvements.

A second set of innovations is equally important. These involve internet-connected end-point protection that makes it possible to distribute through the internet protective software signature code back to devices to identify and disable destructive malware. In a sense, this is a bit like the role radar played in 1940, detecting malware attacks and directing defensive forces to thwart them. MSTIC on repeated occasions has been able to develop new signatures in just a few hours and distribute them back to devices across Ukraine and more globally. These have played a critical role in halting the movement of destructive malware that otherwise could have spread widely across organizations' network domains.

Ongoing wartime measures and innovations with the Ukrainian government have strengthened this protection further. In terms of Microsoft's direct participation, two such measures have been the most important. The first has been the use of technology acquired from RiskIQ that identifies and maps organizational attack surfaces, including devices that are unpatched against known vulnerabilities and therefore are the most susceptible to attack. This information has been shared with the Ukrainian government free of charge to enable it to accelerate the strengthening of cyber-defenses. Ukrainian network defenders worked tirelessly with the constant support of the CERT UA within the government to use this information to protect computers across the country.

The second measure has been a wartime innovation pursued with the collaboration and support of the Ukrainian government. MSTIC recognized that Russian malware could be mitigated meaningfully by turning on a feature in Microsoft Defender called controlled folder access. This typically would require that IT administrators access devices across their organization, work made more difficult and potentially even dangerous in wartime conditions. The Ukrainian government therefore authorized Microsoft through special legal measures to act proactively and remotely to turn on this feature across devices throughout the government and across the country.

Ultimately, all this illustrates three features that characterize the state of cybersecurity protection as we approach the second quarter of the 21st century. The first is the role the private sector now plays in protecting a country in a time of war. Unlike land, sea, and air, cyberspace is owned and operated in part by companies. This makes the war in Ukraine different from major wars of the past. And it imposes a heightened responsibility on tech companies to use the best technology available and sometimes to take extraordinary measures to help defend a country from attack (even at no charge, in the case of Microsoft's support for Ukraine).

Second, this role also places a high responsibility on the tech sector to keep investing in ongoing innovation to ensure that defensive protection not only keeps pace with but exceeds innovations in offensive cyber-attack tactics and capabilities. While it's encouraging to witness the relative success of defensive cyber-security protection in the first four months of the war in Ukraine, in no way can defensive innovations afford to stand still.

Finally, there are important lessons from the war in Ukraine for the cybersecurity protection of all other organizations and individuals around the world. The US Cybersecurity and Infrastructure Security Agency, or CISA, has captured this well in its now-famous phrase "[Shields Up](#)." More than ever, cybersecurity features such as multifactor authentication need to be used by everyone, everywhere. Tech companies like Microsoft will need to continue to make features like these easier for people to use and apply. And organizations and individuals alike will need to make good use of them.

## Russian Network Penetration and Cyber Espionage Activities Outside Ukraine

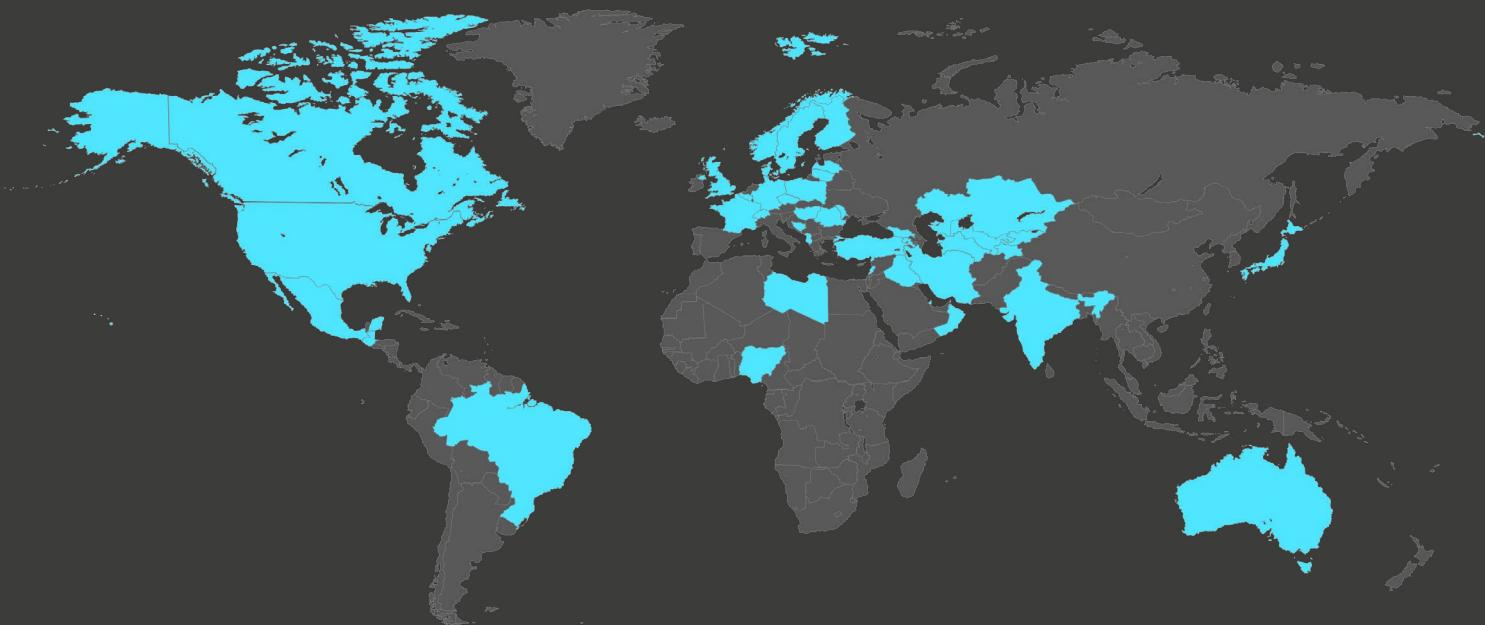
### 3

Destructive cyberattacks represent one part of a broader effort by the Russian government to put its sophisticated cyber capabilities to work to support its war effort. As a coalition of countries has come together to defend Ukraine, Russian intelligence agencies have stepped up their network penetration and espionage activities targeting governments outside Ukraine. Not surprisingly, this increase appears to be most focused on obtaining information from inside the governments that are playing critical roles in the West's response to the war.

Since the war began, MSTIC has detected Russian network intrusion efforts on 128 targets in 42 countries outside

Ukraine. These represent a range of strategic espionage targets likely to be involved in direct or indirect support of Ukraine's defense, 49 percent of which have been government agencies. Another 12 percent have been NGOs that most typically are either think tanks advising on foreign policy or humanitarian groups involved in providing aid to Ukraine's civilian population or support for refugees. The remainder have targeted IT companies and then energy and other companies involved in critical defense or other economic sectors.

#### Countries outside Ukraine targeted by Russian cyber espionage since the start of the war in Ukraine



While these targets are spread around the globe, 63 percent of this observed activity has involved NATO members. Based on MSTIC's observations, Russian cyber espionage efforts have focused on targets in the United States more than any other country, with American targets representing 12 percent of the global total outside Ukraine.

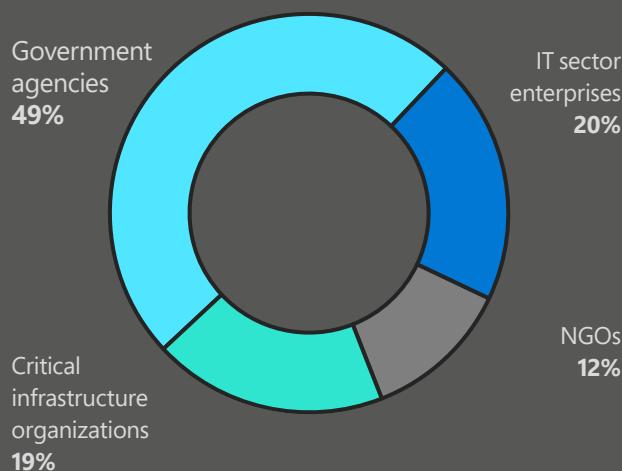
This focus on the United States has been followed closely by activity targeting NATO members that geographically are the closest to Ukraine. At the top of this list is Poland, with 8 percent of intrusions, where the delivery of a majority

of military and humanitarian aid is coordinated. The Baltic countries of Latvia and Lithuania represent a combined 14 percent of total intrusions outside Ukraine. (In contrast, in Estonia, the third Baltic border country, where the country has adopted cloud services, we've detected no Russian cyber intrusions since the onset of the Ukraine war.)

Russian cyber activities have also actively targeted Denmark, Norway, Finland, and Sweden. These collectively represent nearly 16 percent of all the observed Russian attacks globally.

## Recent Russian network penetration and cyber espionage operations outside Ukraine

Russian network intrusion targets



**128** Russian network intrusions

**42** Countries

**29%** Success rate

In most instances the victims were operating on premises, not in the cloud.

Since the start of the war in Ukraine, MSTIC's detections have found that Russian actors have been successful 29 percent of the time. In a quarter of these successful intrusions, MSTIC identified incidents that led to the successful exfiltration of an organization's data.

Microsoft notifies customers when we observe a nation-state attack against them, regardless of whether the attack was successful. These efforts to promptly notify victims of these breaches likely led to the successful defense of their networks. But in most instances the victims were operating on local servers, not in the cloud. As a result, our visibility into the total number of attacks, the success rate, and in particular the extent of data exfiltration, likely understates

the extent of Russian cyber espionage success.

All this reflects the current and global state of offensive cyber espionage and defensive cyber protection. As the SolarWinds incident demonstrated 18 months ago, Russia's intelligence agencies have extremely sophisticated capabilities to implant code and operate as an APT that can obtain and exfiltrate sensitive information from a network on an ongoing basis. There have been substantial advances in defensive protection since that time, especially in cloud services and cloud security technology, but the implementation of these advances remains uneven, especially among European governments. As a result, significant collective defensive weaknesses remain.

## Russian Cyber Influence Operations

# 4

The war in Ukraine has brought into bold relief a third connected aspect of Russia's sophisticated cyber operations. In addition to destructive cyberattacks and cyber espionage efforts, Russian agencies are deploying cyber influence operations that are designed to support its war aims. These involve sophisticated and coordinated efforts to use digital technologies and the internet to create and spread false narratives to advance multiple goals. The longer the war lasts, the more pronounced and important these operations likely will become, especially if they can be used successfully to undermine help Western unity and support.

Foreign influence operations are not new. Nations have used propaganda to further their goals for centuries.

The Soviet Union long invested in and even excelled in sowing doubt, chaos, or confusion in other countries. One of numerous examples involved work in the early 1980s to blame the United States for the spread of AIDS. For example, in July of 1983, an anonymous letter appeared in *The Patriot*, an obscure Indian newspaper. The letter's headline was "AIDS may invade India: Mysterious disease caused by US experiments." The author purported to be a "well-known American scientist and anthropologist" who claimed that the AIDS epidemic was the result of an experiment at the Pentagon. The letter stated that the United States was moving its lab operations to Pakistan, thus putting the Indian people at greater risk.

The letter was later traced back and attributed to the KGB. It was part of a broader campaign that became known as "Operation Infektion." It became one of the most effective foreign influence operations in history. Unaware of the letter's origin, it led to panic by readers who found enough accurate information in it to believe the entire premise was

## Russian information operations in the 1980s

### *AIDS may invade India*

#### Mystery disease caused by US experiments

NEW YORK:

Aids, the deadly mysterious disease which has caused havoc in the US, is believed to be the result of the US government experiments to develop new and dangerous biological weapons.

Now that these menacing experiments seem to have gone out of control, plans are being hatched to move the transfers from the US to other countries, primarily developing nations where governments are pliable to Washington's pressures and persuasion.

Some American experts believe that Pakistan may become the main testing ground for these experiments. If this happens, there will be a real danger that aids may rapidly spread to India with the grave consequences to the people of the country.

WHO representatives point out that aids may soon become problem number one, since so far there are no effective cures to fight it.

The British mass media has pointed to the blood plasma imports from the US as the cause of aids, which is spreading in the British Isles, where more than 100 patients have been hospitalized, with half of them now dead.

As a result, France and Holland, which use large quantities of American blood donations, have stopped importing such blood. Britain, the Federal Republic of Germany and Denmark are now considering similar measures.

In recent months, there has been a marked increase in the incidence of this hitherto unknown disease, the so-called Acquired Immune Deficiency Syndrome (Aids), caused by a scientist suspect, by a new highly pathogenic virus which ravages the immune system of a human being, making him practically defenseless against any infection. Once the aids virus penetrates the human organism, it does not become the "killer" but rather acts like a time bomb. The immune system destroyed by it can no longer resist diseases even such as the virus flu. As a result, many

among immigrants from Haiti. At that time, however, no one seemed to bother to pay any serious attention both on the part of the local authorities and the US public at large. In 1980 there was another sign of aids and it was in New York this time in addition to Haitian immigrants the disease struck local Americans, primarily drug addicts and homosexuals. By February 1981, aids had infected large sections of the American population and had been registered in 33 states. New York accounted for 49 per cent of all the cases that had been officially registered in the US by that time.

Concerned American citizens and organisations began to wonder why does aids, just like some other previously unknown diseases such as bizarre pneumonia or the so-called Legionnaire's disease,

continued on page 7 col. 2



SUNDAY, JULY 17

#### Guerillas And Gorillas

Understanding the reasons why even after a century of political independence the Latin American countries have both their politics deformed and their economy distorted will help to have a better idea of the problems which any post-colonial society faces, writes M. P. Kavalam.

#### Ramadan In Dubai

Perhaps at no time of the year does Dubai come to the fore as a Muslim city than at Ramadan. For the Arabs, the months of fasting apart from being a deeply religious occasion assumes almost a festive air, writes Rashmi Taneja.

OTHER FEATURES : Public View, Nostalgia, Encounters, Thinking One-dimensionally, Short Story by Bandana Majumdar, Education, Mirros/Windows, Film focus, Culture Watch, Sports...

From: History, Philosophy, and Newspaper Library at the University of Illinois at Urbana Champaign

plausible. This is part of the recipe for what has long made for effective Russian influence operations. They are carefully planned to support a broader government strategy, executed with operational patience, take advantage of a specific public issue or concern, and build narratives that combine enough true facts to make a false narrative seem plausible.

And all this was before the internet.

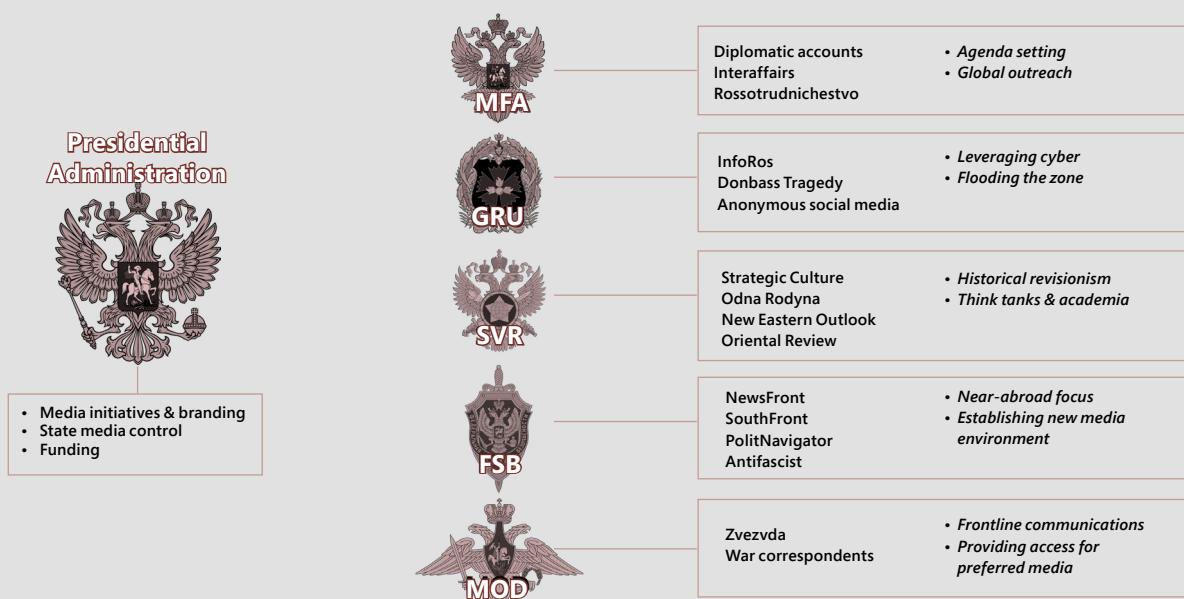
To support the war in Ukraine, the Russian government is deploying a new generation of technology and tactics to support cyber influence operations. These combine traditional tactics with the use of digital technologies and the internet to give foreign influence operations a broader geographic reach, higher volume, more precise targeting, and far greater speed and agility. And, unfortunately, especially when pursued with patience and persistence, these cyber influence operations are almost perfectly positioned to take advantage of the longstanding openness of democratic societies and the public polarization that is characteristic of current times.

The Russian government currently is deploying an expanding cyber influence operation to support its war efforts in Ukraine. These appear to be focused on four distinct audiences. They target the domestic Russian population with the goal of sustaining support for the war by portraying Ukraine's military as responsible for the

conflict. They target the Ukrainian population with the goal of undermining confidence in the country's willingness and ability to withstand Russian attacks. They target American and European audiences to diminish Western unity and deflect criticism of Russian military war crimes. And they target nonaligned countries to support Russian efforts at the United Nations and in other venues, combining longstanding narratives demonizing democracy and Western intentions and with emerging efforts to blame the west for potential food shortages.

Agencies across the Russian government are targeting each audience in textbook fashion through cyber influence operations. These use some tactics that are like those Microsoft has long observed in other Russian cyber activities. As a result and as discussed below, it has become apparent that it will take new digital technologies and the advanced use of data to better detect and counter these operations.

## Russian government's cyber influence operations



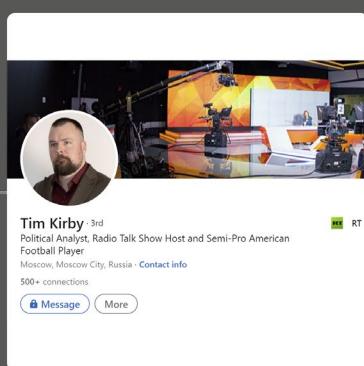
A few examples help illustrate ongoing Russian tactics. Like the patient pre-positioning of malware within an organization's computer network, Russian cyber influence operations pre-position false narratives in the public domain on the internet. This pre-positioning has long helped more traditional Russian cyber activities, especially if IT administrators scan their most recent network activity. Malware that sits dormant for an extended time on a network therefore can make its subsequent use more effective. And false narratives that sit unnoticed on the internet can make subsequent references to them seem more credible.

This approach is part of the reason cybersecurity experts refer to Russian and other intelligence agencies as APTs. In a similar way, Russian agencies operate through APM teams first to plant and subsequently spread their narratives. These teams are pre-positioning false narratives, launching coordinated campaigns to report narratives through government-backed and influencer outlets and channels, and amplifying narratives through tools designed to exploit social media and the internet.

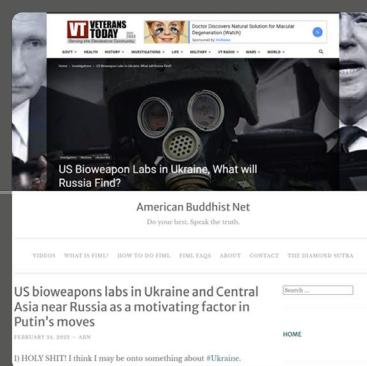
This approach was applied beginning in late 2021 to support the Russian false narrative around purported bioweapons and biolabs in Ukraine. This narrative was first uploaded on to YouTube on November 29, 2021, as part of a regular English-language show by a Moscow-based American expatriate who claimed that US-funded biolabs in Ukraine were connected to bioweapons. The story went largely unnoticed for months. On February 24, 2022, just as Russian tanks crossed the border, this narrative was sent into battle. A data analytics team at Microsoft has identified 10 Russian-controlled or influenced news sites that simultaneously published reports on February 24 pointing back to "last year's report" and seeking to give it credence. Russian-sponsored teams then worked to amplify the narrative on social media and internet sites more broadly.

In recent months, we have used data analytics and new data sets to better track the flow and impact of Russian cyber influence operations. Using these techniques, the Microsoft team identified more than 300 Russian-sponsored websites that published within two weeks stories promoting the biolabs narrative.

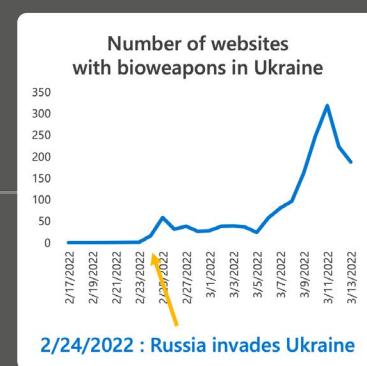
## Bioweapons campaign timeline



November 29, 2021



February 24, 2022



March 11, 2022

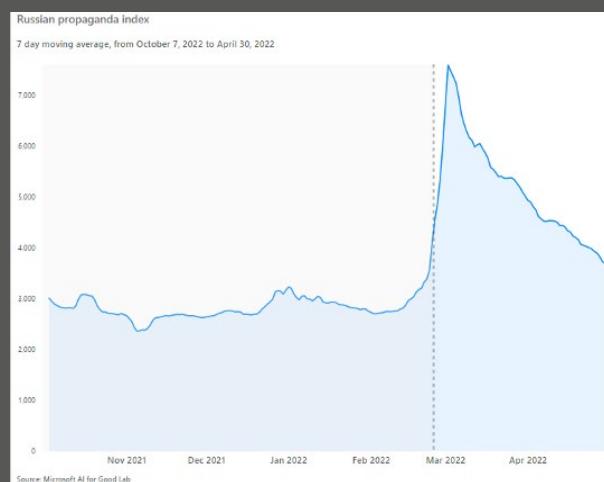
Russian teams subsequently have used these tactics in similar ways, albeit on a rushed wartime basis that reflects less time to plan. As illustrated in an additional example, on March 7, 2022, the Russians published online with the Permanent Mission of the Russian Federation to the UN a claim that a maternity hospital in Mariupol had been emptied and was now being used as a military site. On March 9, two days later, the Russian military bombed the hospital. When UN officials reacted with concern, a Russian representative immediately tweeted that the concern was “fake news,” citing the prior report.

Looking beyond these examples, it’s possible to track and calculate the creation and consumption of Russian propaganda more broadly. Microsoft’s AI for Good Lab has created a Russian Propaganda Index (RPI) to monitor the flow of news from Russian state-controlled and -sponsored news outlets and amplifiers. This index measures the proportion of this propaganda flow to overall news traffic on the internet, and is enabled for geographical regions, online channels, and infrastructure providers such as registrars and

webhosts. The Lab has also developed AI tools to detect new propaganda sites as they appear, using data from a wide variety of internet sources and other identifying characteristics to determine and forecast which new domains may be candidates for foreign cyber influence operations. This technology is used in conjunction with sources from third-party reviewers, such as NewsGuard, and the Global Disinformation Index (GDI) to help us define which sites are known purveyors of state-sponsored media.

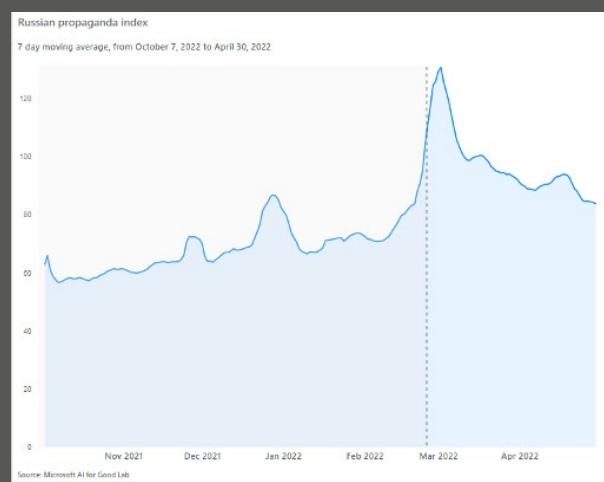
Using these techniques, the RPI can be used to chart the consumption of Russian propaganda across the internet and in different geographies on a precise timeline. The two graphs below show that consumption of narratives from Russian-controlled and -sponsored sites across the internet rose sharply in both Ukraine and the United States in the initial weeks after the war began. The surge in Ukraine represents an increase of 216 percent, while the spread of Russian propaganda in the United States increased by 82 percent.

## Russian propaganda consumption in Ukraine



- Starting in the last week of February, Russian Propaganda Index went up 216% in Ukraine.
- Propaganda peaked on March 2 and has been going down, but is still higher compared to before the war.

## Russian propaganda consumption in the US



- Starting in January 2022, we saw a significant increase in traffic to Russian propaganda websites.
- The amount of Russian propaganda consumption peaked on February 24 with an increase of 82%.
- Even after all efforts to reduce traffic to Sputniknews and RT.com, consumption of Russian propaganda is still higher than before the war (~60MM per month in the US, on par with the WSJ).

Using internet data and these techniques, it's also possible to identify the social media, search, and other sites that are being used to encourage and channel traffic to these stories. And it's possible to identify, as shown below, the specific reports and narratives that attain the highest consumption levels in specific geographies and time periods.

## Top 5 Russian propaganda articles in the US based on visits (February)

**1**

24 Feb. 2022 18:32 | Home | Russia & EEU

**Russian military attack on Ukraine: got there**

Moscow says the current situation is the result of years of failed bloodshed in eastern Ukraine after the 2014 coup in Kiev



### Article justifying the attack on February 24.

"The escalation follows years of unsuccessful talks, broken ceasefire agreements, and a standoff between Russia and the West linked to the 2014 coup that overthrew the government in Kiev."

**2**

24 Feb. 2022 01:02 | Home | Russia & EEU

**Twelve thousand Chechens ready to deploy to Ukraine – Kadyrov**

Chechen fighters support Moscow's intervention in the eastern European nation, the region's chief claims



Thousands of men from Chechnya are arriving to offer assistance to their southern republic's leader, Russian Kadyrov, has pledged, as Moscow's military conducted their second day of strikes in Ukraine.

On Friday, 12,000 local volunteers amassed on the central square of the regional capital, Grozny. Kadyrov informed the publication 'Chechnya Sevodnya' of their rally, which was organized to show their support for the Kremlin and their readiness to aid its objectives.

These are volunteers who are ready to leave for any special operation at any time in order to

### Article about 12k volunteer Chechen soldiers ready to fight in Ukraine.

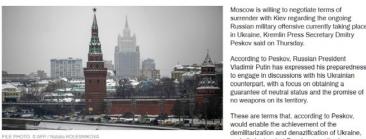
"On Friday, 12,000 local volunteers amassed on the central square of the regional capital, Grozny. Kadyrov informed the publication 'Chechnya Sevodnya' of their rally, which was organized to show their support for the Kremlin and their readiness to aid its objectives."

**3**

24 Feb. 2022 01:02 | Home | Russia & EEU

**Russia ready to negotiate with Ukraine – Kremlin**

The Kremlin presents Kiev with two demands



Moscow is willing to negotiate terms of war with Kiev regarding the ongoing Russian military offensive currently taking place in Ukraine, Russian Press Secretary Dmitry Peskov said on Friday.

According to Peskov, Russian President Vladimir Putin has expressed his preparedness to engage in discussions with his Ukrainian counterpart, with a focus on obtaining a guarantee of neutral status and the promise of no weapons on its territory.

These are terms that, according to Peskov, would enable the achievement of the de-territorialization and denazification of Ukraine, and ultimate withdrawal from areas as

### Article about terms of surrender from Ukraine.

"According to Peskov, Russian President Vladimir Putin has expressed his preparedness to engage in discussions with his Ukrainian counterpart, with a focus on obtaining a guarantee of neutral status and the promise of no weapons on its territory."

**4**

24 Feb. 2022 01:02 | Home | Russia & EEU

**How Ukraine's 'Revolution of Dignity' led to war, poverty and the rise of the far right**

A motley crew of militant Ukrainian nationalists and pro-Western activists wanted to change their democratically elected government. Eight years on, the results look disappointing.



### Article about how Ukraine's revolution led to war.

"A motley crew of militant Ukrainian nationalists and pro-Western activists wanted to change their democratically elected government. Eight years on, the results look disappointing."

**5**

24 Feb. 2022 01:02 | Home | Russia & EEU

**Ukraine ready to discuss neutrality, Zelensky says**

The Ukrainian president says Kiev has been left to fend for itself as NATO is "afraid" to give it any guarantees



Accusing the West of leaving Ukraine to face Moscow alone, President Volodymyr Zelensky said on Friday he was not afraid to negotiate an end to the Russian 'invasion,' but would need security guarantees to do so.

Speaking in the early hours of the morning from Kiev, Zelensky said he had reached out to Joe Biden to tell him that Ukraine's 'time was at stake.'

'They [the West] are you with us?' Zelensky said. 'They aren't. They are afraid. They don't want to take on any risk. The allies are afraid. 27 members of Europe, if Ukraine will be in NATO, they will be afraid. They will not respond.'

### Article about how the West will not help Ukraine.

"Accusing the West of leaving Ukraine to face Moscow alone, President Volodymyr Zelensky said on Friday he was not afraid to negotiate an end to the Russian 'invasion,' but would need security guarantees to do so."

From: February 1-28, 2022

In part, as shown above, the sharp rise in February appears to reflect some months of planning for selected narratives. But as shown on the graphs above, the tech sector's efforts in early March to curtail the amplification of narratives from RT and Sputnik likely helped reduce the spread of Russian propaganda back to pre-February levels. And, as mentioned above, the onset of war likely has led subsequently to more hurried Russian activities that are less planful and patient.

Notably, however, the broader RPI levels in the United States and Ukraine both remain at pre-February levels. And these levels, which reflect a steady flow of Russian cyber influence operations, remain substantial. For example, this reflects an estimated average American consumption of Russian propaganda 60 million to 80 million page views per month, enough to make the collective placement resulting from Russian cyber influence on par with a major publication like the Wall Street Journal in the United States. And this estimate of Russian propaganda almost certainly understates its total reach, given the inability at this point to ascertain with confidence and include every outlet being used.

This reflects in turn the many years that Russian cyber influence operations have been growing. These are not confined to a single issue or country. For example, using similar digital and AI tools and the use of broader data sets, it's possible to look back and better assess the breadth and depth of Russian cyber influence operations focused on COVID-19 vaccine and lockdown issues. Russian efforts include a broad multilingual approach, with outlets such as RT and Sputnik publishing initial content in more than 20 languages.

The expanded use of public data illuminates the extraordinary contrast in vaccine messaging on a site like RT. For example, the most widely accessed relevant story on RT in Russian suggested that lockdowns and booster shots prevent COVID-19 transmission, while the most widely accessed story in English asserted that vaccinations fail to curb transmission and are ineffective against new strains. While democratic societies rely on the public to discern what is true and what is false, logic makes plain that both these stories cannot possibly be true at the same time.

## Russian COVID-19 messaging differs by language Anti-vaccine propaganda targets non-Russian readers

Topics covered by **top 10 most-viewed** coronavirus stories on RT.com

### Russian (*Translated below to English*)

- "Lockdowns & boosters prevent transmission"
- "Russian public figures are testing positive"
- "Cases & deaths are increasing in Russia"
- "The Sputnik V vaccine is highly effective"
- "Vaccine proof needed on public transport"

*"Chief Physician of the Center for Public Health and Medical Prevention of the Yamalo-Nenets Autonomous Okrug supported the idea of **mandatory vaccination** against COVID-19 for certain population groups."*

Source: <https://ru.rt.com/jqtq>

*"The most **critical situation** with mortality, hospitalization, and the proportion of seriously ill patients on artificial lung ventilation is noted in the Kursk region... Golikova said."* Source: <https://ru.rt.com/jpge>

### English

- "Vaccinations fail to curb transmission and are ineffective against new strains"
- "Pfizer vaccine has dangerous side effects"
- "Mass vaccination is politically motivated"
- "Pfizer & Moderna conduct unregulated trials"

*Documents released by the Food and Drug Administration reveal that drugmaker Pfizer recorded nearly **160,000 adverse reactions** to its Covid-19 vaccine in the initial months of its rollout." Source: <https://on.rt.com/bmzd>*

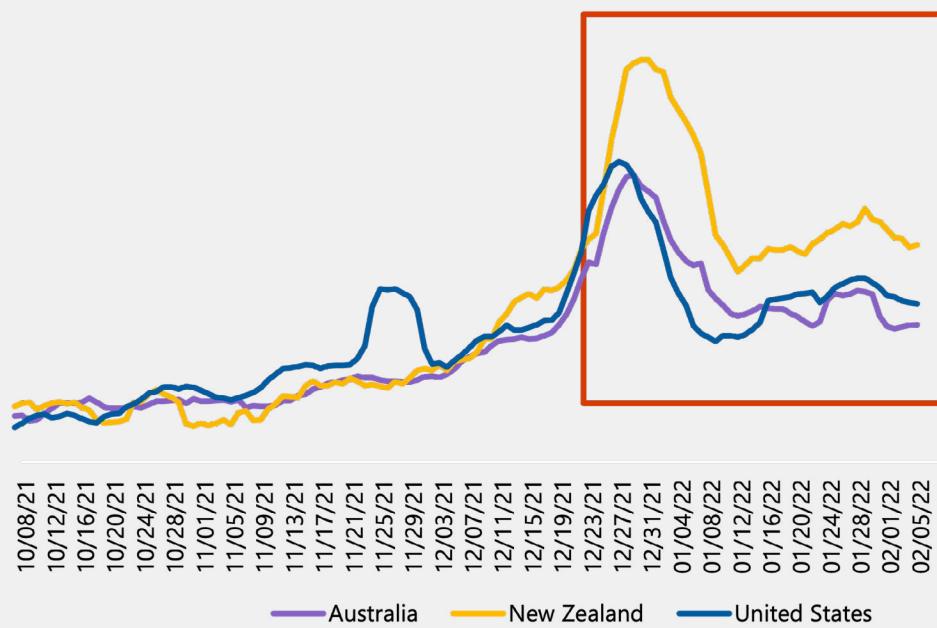
*"Successful vaccine rollouts have **failed to stop Covid transmission**, with new data showing the prevalence of the virus increasing in fully jabbed individuals, according to a medical study in The Lancet." Source: <https://on.rt.com/bm4s>*

From: October 1, 2021 – April 30, 2022

## New Zealand

This comparison also reflects the global reach of Russian cyber influence operations, with what appears to be more localized planning and impact. For example, Microsoft's RPI numbers for New Zealand show a spike beginning in December 2021 that exceeds the figures for Australia the United States.

### Russian Propaganda Index (RPI), New Zealand vs Australia and US



Russian propaganda consumption in New Zealand is similar to Australia until the first week of December 2021.

**After December, Russian propaganda consumption in New Zealand increased** by over 30% relative to consumption in Australia and the US.

An assessment of the stories driving Russian propaganda consumption in New Zealand in late 2021, including below, shows a clear focus on COVID-19 issues. The top two stories, for example, drove narratives that questioned the efficacy of vaccines and suggested that they had life-threatening side effects. While it would be premature to draw concrete conclusions at this point about cause and effect, this spike in Russian propaganda consumption in New Zealand preceded an increase in public protests in early 2022 in Wellington, the nation's capital.

## Top 5 Russian propaganda articles in New Zealand based on visits (October-December)

**1**

**"Most vaccinated" place on earth cancels Christmas**



A surge in Covid-19 cases, Gibraltar has canceled official Christmas events and 'strongly' discouraged people from hosting private gatherings for four weeks. Gibraltar's entire eligible population is vaccinated.

The drastic increase in the numbers of people testing positive for Covid-19 in recent days is a stark reminder that we must remain very vigilant as a community and that it is the

### Article questioning the value of vaccines.

"Amid a surge in Covid-19 cases, Gibraltar has canceled official Christmas events and 'strongly' discouraged people from hosting private gatherings for four weeks. Gibraltar's entire eligible population is vaccinated."

**2**

**High Recorded Mortality in Countries Categorized as "Covid-19 Vaccine Champions". The Vaccinated Suffer from Increased Risk of Mortality**



Data on Mortality in the Most Vaccinated Countries. Increases Hospitalizations of the Vaccinated

Since the beginning of the health crisis, the French government has claimed that each measure was effective. It has imposed major restrictions on our freedom, in particular on doctors' prescriptions. It has also promised that vaccination would achieve collective immunity by the end of the crisis and return to normal. But the failure of 18 months of the so-called 'health strategy' based on false simulations, innumerable lies, promises never kept, as well as the propaganda and fear campaign has become unbearable.

Are the current vaccines that they want to impose on us effective? Failure for 18 months of this so-called 'health strategy' based on false simulations, innumerable lies, promises never kept, as well as the propaganda and fear campaign has become unbearable.

### Article about how those vaccinated suffer from increased risk of mortality.

"Are the current vaccines that they want to impose on us effective? Failure for 18 months of this so-called 'health strategy' based on false simulations, innumerable lies, promises never kept, as well as the propaganda and fear campaign has become unbearable."

**3**

**Video: A Final Warning to Humanity from Former Pfizer Chief Scientist Michael Yeadon**



All Global Research articles can be read in 57 languages by activating the "Translate Website" drop down menu on the top banner of our home page (Desktop version).  
Visit and follow us on Instagram @GRC\_globalresearch  
...  
First posted on September 30, 2021  
Written by Dr. Michael Yeadon  
Former Vice President and Chief Science Officer of Pfizer, talking about the pandemic and the COVID vaccine

### Article about ex-Pfizer scientist Michael Yeadon who became an anti-vaxxer.

"You don't need vaccines and you don't need any of the measures that have been introduced... and yet governments and their scientific advisors have lied to us for a year... And just produced mayhem."

**4**

**Pfizer documents reveal variety of vaccine side effects**



Documents released by the Food and Drug Administration (FDA) reveal that nearly 1.2 million Americans experienced at least 160,000 adverse reactions to its Covid-19 vaccine in the first six months.

The documents were obtained by a group of doctors, professors, and journalists calling themselves Public Health Transparency, which filed a Freedom of Information Act (FOIA) request with the FDA for them.

The first tranche of documents reveal that, as of February 2021, when Pfizer's shot was being rolled out worldwide on an emergency basis, the

### Article about Pfizer vaccine side effects and deaths.

"These reactions ranged from the mild to the severe, and 1,223 were fatal. The majority of these case reports involved people aged between 31 and 50 in the United States."

**5**

**Pfizer admits to using aborted fetal tissue in developing its vaccines. So can Christians sign up for a jab exemption now?**



Robert Bridgeman, an American writer and journalist, is the author of *Murder in the American Dream: How Corporations and Their Political Servants are Destroying the American Dream*.

### Article claiming Pfizer admitted to using aborted fetal tissues in vaccines.

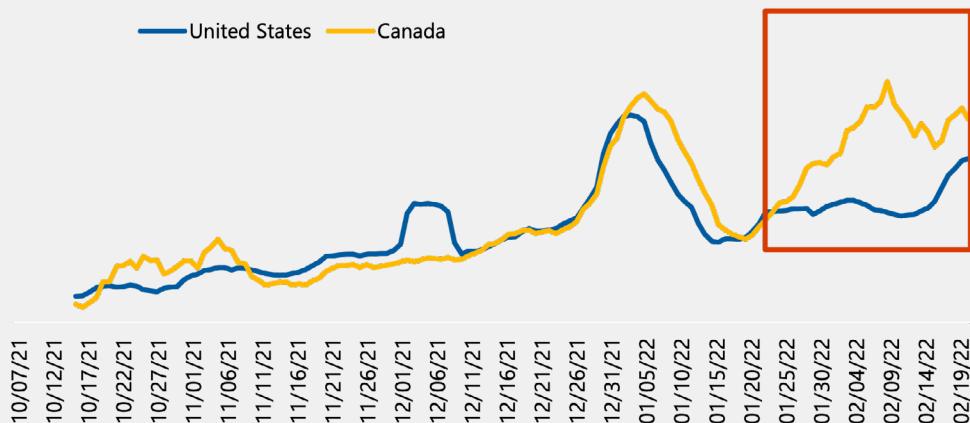
"For billions of faithful around the world, abortion is considered first-degree murder, yet fetal tissue is being used to develop Covid vaccines. While some may argue that 'killing a life to save millions' is fine, many disagree."

From: October-December 2021

## Canada

A similar picture emerges from the RPI figures in Canada. Not surprisingly, the trend lines in Canada and the United States typically move in tandem. But earlier this year they diverged starting on January 18, with the reach of Russian propaganda peaking in Canada on February 5.

### Russian Propaganda Index (normalized) US vs Canada



Russian propaganda in Canada had a similar trend compared to the US until the last week of January.

**Russian propaganda increased ~20% in Canada relative to the US from 1/20/2022 to 2/18/2022.**

Microsoft's data found that four of the five most widely read internet-based propaganda stories in Canada in this period focused on COVID-related protests in Ottawa. These reflected in part on a propaganda narrative suggesting that mainstream media coverage of these protests was inadequate or biased. The start of this surge preceded the arrival of a large convoy of protestors in trucks in Ottawa on January 28. Protestors then occupied areas around the Parliament building the last week of January and the first week of February, and the protests expanded to the Canadian-US border and disrupted trade on February 8, just after propaganda dissemination reached its peak.

## Top 5 Russian propaganda articles in Canada based on visits (January 20 – February 7)

**1 Canadian capital declares state of emergency over Freedom Convoy**

Ottawa mayor seeks federal assistance, insisting anti-Covid-mandate protest is out of control



Ottawa mayor Jim Watson has declared a state of emergency, citing 'serious danger and threat to the safety and security of residents.' As Freedom Convoy truckers and their pedestrian supporters continue to occupy the capital, the mayor said he had been 'concerned by the situation Sunday that police have been outnumbered by the demonstrators' and indicated he wants the RCMP to take over security of the protest site. 'The situation at this point is completely out of control because the individuals with the protest are more numerous than we have police officers and I've indicated to the other that ...'

### Article that describes when Ottawa declared state of emergency.

"Ottawa mayor Jim Watson has declared a state of emergency, citing 'serious danger and threat to the safety and security of residents,' as Freedom Convoy truckers and their pedestrian supporters continue to occupy the capital."

**2 Canada's Freedom Convoy Demolished – CIA Colour Revolutions Celebrated**

By Sam O’Hearn | Jan 29, 2022 | 11:45 AM EST | Updated: Jan 29, 2022 | 11:45 AM EST



All Global Research articles can be read in 11 languages by selecting the "Translate Website" drop down menu on the top right. To receive Global Research's Daily Newsletter (subjected articles), click here.

Since the 27th of January, despite receiving no mainstream media coverage whatsoever, Protests of Canadian truck drivers and their supporters continued in a major Canadian city, a clear violation of a new protocol in response to the Canadian government's decision to ban the already authorized Convoy protesters by mandating that truck drivers in every Canadian town the federal agency responsible for the transport of goods across the country must wear a mask and practice physical distancing. This is the latest in a series of measures taken by the Canadian government to combat the spread of the Omicron variant of the coronavirus, which has been highlighted by Prime Minister Justin Trudeau as one of the country's "greatest threats" during a 2021 conference.

With the Freedom Convoy converging on the Canadian capital Ottawa on Saturday January 29th, however, the week-long media silence on the protest disappeared only to be quickly replaced by widespread mainstream media condemnation.

READ MORE: Kazakhstan and Europe's Anti-lockdown Protest – A Contrast In Reactions

### Article states that protests in Canada received no mainstream media coverage.

"With the Freedom Convoy converging on the Canadian capital Ottawa on Saturday January 29th, however, the week-long media silence on the protest disappeared only to be quickly replaced by widespread mainstream media condemnation."

**3 Canada's Freedom Convoy has perfectly exposed legacy media's concealed bias**

By Michael Cheung | a political and cultural commentator. His work has been featured in The Globe, The Intercept, Human Events, and The Real News.



The Freedom Convoy, which set out from British Columbia on January 27th, has been welcomed by Canadian truckers driving across the country to protest the government's Covid-19 'Canadian truckers rule,' Musk tweeted on Thursday afternoon.

The Freedom Convoy will set out from the Canadian capital of Ottawa sometime this weekend, according to Musk, who has already called out first. As it approached Ontario,

### Article about mainstream media being biased.

"News organizations that promised not to allow democracy to 'die in darkness' have instead become the very penumbra obscuring the truth."

**4 Joe Rogan, Elon Musk react to Canadian trucker convoy**

'Freedom convoy' denied by PM Justin Trudeau finds major attention south of the border



Trucks and drivers from the Freedom Convoy and podcaster Joe Rogan have rallied outside the Canadian Parliament in Ottawa, Canada, on Thursday afternoon, after Prime Minister Justin Trudeau denounced them as a 'fringe minority' with 'unacceptable attitudes.'

'Canadian afternoon,' Musk tweeted on Thursday afternoon.

The Freedom Convoy, which set out from British Columbia on January 27th, has been welcomed by Canadian truckers driving across the country to protest the government's Covid-19 'Canadian truckers rule,' Musk tweeted on Thursday afternoon.

### Article about support of Elon Musk and Joe Rogan to Canadian truckers.

"Tesla and SpaceX founder Elon Musk and podcaster Joe Rogan have spoken about the Canadian truckers driving across the country to protest the government's Covid-19 'Canadian truckers rule,' Musk tweeted on Thursday afternoon."

**5 'Major non-NATO ally' loses US military aid**

The cancellation of American military assistance to Egypt comes just days after a \$2.5 billion arms deal was agreed between the two nations.



The US has announced that it is canceling \$130 million in military aid to Egypt over human rights concerns, with the move coming just days after the Biden administration approved a \$2.5 billion arms sale to the North African country.

Cairo has failed to meet all the human rights benchmarks required for the \$130 million in military aid, according to the US State Department, announced on Friday.

The US has also decided to postpone its planned security review to re-examine the \$2.5 billion in other national security priorities. "It turned out, when we did our review, that there were some significant gaps,"

In September, Secretary of State Antony Blinken announced \$130 million in foreign military aid to Egypt, but withheld another \$1.35 million on

### Article about the cancellation of American military assistance to Egypt.

"The US has announced that it is canceling \$130 million in military aid to Egypt over human rights concerns, with the move coming just days after the Biden administration approved a \$2.5 billion arms sale to the North African country."

From: January 20 – February 7, 2022

All of this is indicative of the global reach of Russian cyber influence operations. These efforts rely fundamentally on digital technology. They also rely on unintended action by enablers across the tech ecosystem. These include companies that register internet domains, host web sites, promote material on social media and search sites, and channel traffic and help pay for these exercises through digital advertising. It therefore will be important to better assess the role of the tech sector in connection with these operations. There is a growing danger that Russian cyber influence operations will seek to exploit all these resources

to support a longer war in Ukraine. The longer the war, the more challenging it may become to sustain the unity and commitment of a broad international coalition. Just as Russian operations focused during the past year on COVID-19 fatigue, Ukraine and its NATO and other allies will need to prepare for Russian efforts to use cyber influence operations to undermine the support of their publics for Ukraine. And as discussed below, like all the other threats based on cyber technologies, the work to counter these threats will require new innovations in both technology and public-private collaboration.

## A Strategic Response to the Full Range of Russian Cyber Threats

# 5

Perhaps more than anything, the lessons from Ukraine call for a coordinated and comprehensive multilateral and multistakeholder strategy to strengthen defenses against the full range of Russian cyber destructive, espionage, and influence operations. It's perhaps too easy for those outside of Russia to view these three areas as falling into separate silos. But it's helpful to recall the lessons that the British author and journalist Gillian Tett documented more broadly in her book "The Silo Effect." Notably, when people put problems and issues in different categories, they more likely will fail to connect the dots between them. In this case, analytical fragmentation creates the risk of tunnel vision for different cyber defenses and creates opportunities for foreign adversaries to exploit the seams between disconnected defensive efforts.

In fact, new advances in the defense of all these cyber threats will depend on some common tenets and, at least at a high level, a common strategy. The first defensive tenet should recognize that Russian cyber threats are being advanced by a common set of actors inside and outside the Russian government that rely on similar digital tactics. For example, the same agencies play overlapping roles in cyber destructive, espionage, and influence operations. And while it's possible to find encouragement in either some Russian missteps or early triumphs of defensive technology, the easiest and biggest mistake would be to declare a premature victory. Wars are won over time, setbacks can be reversed, and Russian agencies have long invested in sophisticated cyber tactics and techniques.

### Four tenets to counter Russian cyber threats

#### Digital tactics

Recognize that Russian cyber threats are being advanced by a common set of actors inside and outside the Russian government and rely on similar digital tactics. Use digital technology and tactics to help counter them.

#### Public-private collaboration

Recognize that unlike the traditional threats of the past, cyber defenses require a unique level of public and private collaboration.

#### Multilateralism

Embrace the need for close and common multilateral collaboration among governments to protect open and democratic societies.

#### Free expression

Uphold the importance of creativity and free expression in democratic societies, even as new steps are needed to address the full range of cyber threats.

A second defensive tenet should recognize that unlike the traditional threats of the past, cyber defenses rely on a unique level of public and private collaboration. The evolving threat landscape requires a whole-of-society approach. The private sector, particularly technology companies, are on the front lines of cyber and information attacks. Likewise, civil society organizations are key conveners that play a crucial role in engagement, sometimes are involved in cyber data analysis, and are often targets of these campaigns themselves.

The fact that this report is authored by a company is clear evidence of the inevitable role that the technology sector plays in the cyber defense of nations in the world today. There is no ability to deny the importance of this role. There is only the question of whether it will be done well, and this requires both that leading technology companies adapt and that governments work with the private sector in new ways.

A third defensive tenet should embrace the need for close and common multilateral collaboration among governments to protect their open and democratic societies. While Russia's destructive cyberattacks have been confined to Ukrainian territory, the other cyber aspects of the war have a far wider reach. As this report shows, the defense of Ukraine has depended critically on its ability to move data while accessing it beyond its own borders. When one considers the combination of cyber espionage and cyber influence operations, it's apparent that the

world's democracies share both common strengths and vulnerabilities. And the defense of these vulnerabilities will increasingly require a common and united response.

A fourth and final defensive tenet should uphold the importance of creativity and free expression in democratic societies, even as new steps are needed to address the full range of cyber threats. The very definition of free and democratic societies is founded on freedom of expression and the ability of people to create, share, and find content, including material that sometimes reflects sharply contrasting views. Democratic societies view this as a strength rather than a weakness. And since the dawn of the first industrial revolution in the United Kingdom, freedom of thought has stimulated economic and technical innovation as well as new political currents.

**An effective response must build on these tenets with four strategic pillars. These should increase collective capabilities to better (1) detect, (2) defend against, (3) disrupt, and (4) deter foreign cyber threats.** This approach is already reflected in many collective efforts to address destructive cyberattacks and cyber-based espionage. They also apply to the critical and ongoing work needed to address ransomware attacks. We now need a similar and comprehensive approach with new capabilities and defenses when it comes to combatting the growing threat of foreign cyber influence operations. Here the work is less advanced, which is why this is discussed in additional detail below.

## A comprehensive strategy to combat foreign cyber influence operations



The freedom of expression is of distinct importance in developing a strategic response to foreign cyber influence operations. This freedom inherently impacts and even limits the role of democratic governments in addressing any issue associated with content on the internet. It's an element that requires non-partisan discussion and considered thought.

The freedom of expression should also be of comparable importance to the role of tech companies, even as this differs in key respects from the role of governments. To support this, Microsoft has adopted four principles to anchor our work in this space. These start with a first principle that commits us to respect freedom of expression and uphold our customers' ability to create, publish, and search for information via our platforms, products, and services. Second, we will proactively work to prevent our platforms and products from being used to amplify foreign cyber influence sites and content. Third, we will not willfully profit from foreign cyber influence content or actors. And finally, we will prioritize surfacing content to counter foreign cyber influence operations by utilizing internal and trusted third-party data on our products.

**Microsoft has adopted four principles to anchor our work in this space. These start with a first principle that commits us to respect freedom of expression and uphold our customers' ability to create, publish, and search for information via our platforms, products, and services. Second, we will proactively work to prevent our platforms and products from being used to amplify foreign cyber influence sites and content. Third, we will not willfully profit from foreign cyber influence content or actors. And finally, we will prioritize surfacing content to counter foreign cyber influence operations by utilizing internal and trusted third-party data on our products.**

**Detection.** As with cyber defenses, the first step in countering foreign cyber influence operations is building the capacity to detect them. For our part, Microsoft is building on our already mature cyber threat intelligence infrastructure to develop a broader view inclusive of foreign influence operations.

In addition to the digital, AI, and data advances discussed in the preceding section, last week we announced that we entered into an agreement to acquire Miburo Solutions, a leading cyber threat analysis and research company specializing in the detection of and response to foreign cyber influence operations. Miburo's analysts will join Microsoft's cybersecurity teams and play a vital role in expanding our threat detection and analysis capabilities to address new cyberattacks and shed light on the ways in which foreign actors use cyber influence operations in conjunction with other cyberattacks to achieve their objectives.

Of course, no single company or organization can hope to make progress in any of these areas by itself. New and broader collaboration across the tech sector will be important. And progress in analyzing and reporting foreign cyber influence operations will heavily rely on the role of civil society, including in academic institutions and non-profit organizations.

Recognizing this role, researchers Jake Shapiro and Alicia Wanless at Princeton University and the Carnegie Endowment for International Peace respectively have mapped out plans to launch the new "Institute for Research on the Information Environment" (IRIE). With support from Microsoft, the Knight Foundation, and Craig Newmark Philanthropies, this new institute will create an inclusive multi-stakeholder research institution modeled after the European Organization for Nuclear Research (CERN). It will combine expertise in data processing and analysis to speed up and scale new discoveries in this space. Findings from this institute can be used to inform policy makers, technology companies, and consumers more broadly.

**Defense.** The second strategic pillar should shore up democratic defenses. This is a longstanding priority that needs investment and is ripe for innovation. In part this should take account of the challenges technology has created for democracy and the opportunities technology has created to defend democratic societies more effectively.

It's appropriate to start with one of the great technological challenges of our age, which is the impact of the internet and digital advertising on traditional journalism. Since the 1700s, a free and independent press has played a special role in supporting every democracy on the planet. This report appears 50 years and a few days after the Watergate break-in. This makes it even more fitting to recognize the longstanding role of the free press in uncovering corruption, documenting wars, and illuminating the largest societal challenges of this and every other time. But the internet has gutted local news by devouring advertising revenue and luring away paid subscribers. Far too many local newspapers have collapsed, and one of the many insights from our recent work has shown that American counties that lack a newspaper are unknowingly and inevitably exposed to a greater than average share of foreign propaganda, especially from Russia.

For these reasons, one of democracy's critical defensive prongs must strengthen traditional journalism and a free press, especially at the local level. This requires ongoing investment and innovation that must reflect the local needs of different countries and continents. The issues are not easy, and they require multi-stakeholder approaches, which Microsoft and other tech companies increasingly are supporting. They also increasingly involve new innovations in public policy, and this too deserves to become an increasing public priority. This can include laws that enable publishers to negotiate ad revenue collectively with technology companies and legislation that provides tax credits to relieve local newsrooms of a portion of their payroll taxes for journalists they employ.

Journalists also need many other tools for their craft. One is the ability to separate content from legitimate and fraudulent sources. Technology is creating an ability to falsify content and conceal their origin, and the ongoing development of AI that can be used to create "deep fakes" risks making this problem much worse. This makes it important for the technology and media sectors to work together, as they are through the Coalition for Content Provenance and Authenticity (C2PA), to help create the first version of a technical standard that certifies the source and history of media content.

There is also a rapidly evolving need to help consumers develop a more sophisticated ability to identify propaganda that comes from foreign cyber influence operations. While this may seem daunting, in some ways it resembles the work the tech sector has long pursued to combat other cyber threats. Consider the education of consumers to look more carefully at an email address to help spot spam or other fraudulent communications. Countries like Finland and Sweden have for decades educated consumers to help identify Russian propaganda. Initiatives in the United States like the News Literacy Project and the Trusted Journalism Program are helping to develop better informed consumers of news and information. And globally, new technology like the browser plug-in from NewsGuard can help move this effort forward much faster.

This also should remind us that part of the foundation for democracy is an education in civics. As always, this needs to start in schools. But we also live in a world that requires that we all get ongoing civics education throughout our lifetime. The new Civics at Work pledge, led by the Center for Strategic and International Studies, seeks to reinvigorate civics literacy within corporate communities. It's a good example of the breadth of opportunity to strengthen our democratic defenses.

**Disruption.** In recent years, Microsoft’s Digital Crimes Unit has refined tactics and developed tools to help disrupt cyber threats that range from ransomware to botnets and nation-state attacks. We’ve learned many critical lessons from this experience, starting with the role that active disruption can play to counter a broad range of cyberattacks.

As we think about countering foreign cyber influence operations, disruption may play an even more important role. And the best approach to disruption is becoming increasingly clear.

The best antidote to broad deception is more transparency. There is an opportunity to counter foreign efforts to mislead the public by providing the public with better information. (This is part of the reason independent journalism is so important). Efforts to promote transparency through more information not only avoid the understandable concerns and controversies that result from censorship; they build credibility and confidence, especially when a track record gives people the opportunity to assess for themselves information from trustworthy sources.

We have put this type of transparency into action across a range of cyberthreats. For example, it was only a few years ago at Microsoft that we debated internally and then took the first decision to attribute a cyberattack to a nation-state. (It’s perhaps not a coincidence that it involved Russia.) We’ve learned that governments, tech companies, and NGOs should attribute cyberattacks carefully and with ample evidence. But the impact of such disruption is vital, and it has the potential to be even more helpful in disrupting foreign cyber influence. Witness the US government’s information-sharing in the lead-up to Russia’s invasion of Ukraine, exposing Russian plans, including specific campaigns such as a plot to use a fake graphic video, that put transparency into effective action.

Like the recent publication from the CyberPeace Institute in Geneva on ongoing cyberattacks inside and outside Ukraine, there is an opportunity for a broad range of civil society and private-sector organizations to advance transparency

relating to Russia’s cyber influence operations. Reliable reports about newly discovered and well-documented operations can help the public better evaluate what it reads, sees, and hears, perhaps especially on the internet.

To this end, Microsoft will build on and extend its existing cyber reports and will release new reports, data, and updates related to what we discover about Russian cyber influence operations, including attribution statements when appropriate. And starting in late 2022, we will publish an annual report that uses a data-driven approach to look across the company at the prevalence of foreign information operations on our platforms, the efficacy of our ongoing efforts, and next steps to ensure incremental improvement.

It will become important to consider additional steps that can build on this type of transparency. The role of digital advertising is especially important since ads can help fund these foreign operations while in the process helping to create an appearance of legitimacy for foreign-sponsored propaganda sites. Like ransomware, the Russian government has helped foster a cyber influence ecosystem that pursues deception for profit, fueled in part by digital ad revenue. New efforts will be needed to disrupt these financial flows.

**Deterrence.** Finally, we cannot expect nations to change behavior if there is no accountability for violating international rules. Such accountability is uniquely a governmental responsibility. But increasingly, multistakeholder action is playing an important role in strengthening and extending international norms. More than 30 online platforms, advertisers and publishers—including Microsoft—signed on to the recently updated European Commission’s [Code of Practice on Disinformation](#), agreeing to strengthened commitments to tackle this growing challenge. Like the recent Paris Call, the Christchurch Call, and the recent Declaration on the Future of the Internet, multilateral and multistakeholder action can bring together the governments and public among democratic nations. Governments can then build on these norms and laws to advance the accountability the world’s democracies need and deserve.

