The Heritage Foundation

BACKGROUNDER

No. 3704 | APRIL 28, 2022

BORDER SECURITY AND IMMIGRATION CENTER

# U.S. Must Implement Lessons on "Hybrid" Conflict from Ukraine War

*Dustin Carmack*

## KEY TAKEAWAYS

Russia's shadow war that preceded its invasion of Ukraine highlights U.S. vulnerabilities in cyber security, intelligence sharing, technological innovation, and access to independent media.

Russia, China, Iran, and North Korea have weaponized cyberspace, intelligence gathering, informational operations, espionage, communication tactics against the U.S.

The United States must work with our allies and partners to expediently implement lessons-learned from the Ukraine war in order to address future long-term conflicts in this space.

War is a continually evolving architecture, forever changing with the nature of weapons systems, technology, information, and communication development. The Russian invasion of Ukraine is of both a scale and type that the world has not seen in tandem for decades. Kinetic strikes by air and land involving ground troops, tanks, artillery, missiles, and aircraft are happening around the clock throughout the cities and countryside of Ukraine. These actions are readily apparent to spectators around the world. However, a shadow war has been conducted in parallel—advancing ahead of the first tanks to cross Ukrainian borders—and continuing to this day. Russia's hybrid tactics are difficult to see as they occur in cyberspace, intelligence-gathering, informational operations, espionage, communication efforts, and in the darkness of space.

Today such actions are not unique to the current conflict. They serve vital and everchanging roles in active and low-intensity conflict and are generally ambiguous by design. Of note, they include "unconventional tactics, from cyberattacks, to propaganda and political warfare, to economic coercion and sabotage, to sponsorship of armed proxy fighters, to creeping military expansionism."[1] They also frequently include advanced technological and informational strategies to allow small nation-states to punch above their weight in non-conventional warfare and are often difficult to attribute to a particular antagonist. U.S. adversaries, including China, Iran, North Korea, and Russia, have used these tools to various effect against U.S. interests.

Many lessons of the current war will need to be assessed. Policymakers must thoroughly review areas such as conventional warfare, battlefield tactics, motivation and morale, sanctions efforts, and diplomatic approaches in order to prepare for future aggressions. The elements of hybrid warfare that are currently difficult to perceive will take time to unpack and understand. The United States has a slew of vulnerabilities that must be tackled with expedient resolve and must work with allies and partners, both at home and abroad, to build better defenses, intelligence-sharing mechanisms, technological capabilities, information distribution, and resilience.

The Russian war on Ukraine is showing the benefits and limitations of various hybrid capabilities. The U.S. should implement lessons learned in order to address future long-term conflicts and expediently develop countermeasures and solutions that require cooperation from federal, state, and local governments, as well as the private sector.

## Cyber Actions to Date

Leading up to the invasion, Russia and/or its proxies have been identified as the likely culprits behind Ukrainian website defacements, destructive malware, and distributed denial of service (DDoS) attacks, many that began in the weeks leading up to the invasion.[2] Impacted industries included finance, defense, and aviation sectors, and attacks spilled over to several linked organizations in Lithuania and Latvia.[3] Russian military hackers were identified and thwarted recently by Ukrainian cyber response teams after attempts to infiltrate Ukrainian power substations that could have caused 2 million people to lose power.[4]

To date, however, large-scale cyber and electronic warfare attacks have not been seen or fully known—yet. Russia knocked out parts of Ukraine's power grid in 2015 and 2016 and unleashed the 2017 destructive NotPetya malware attack that impacted the globe, causing billions of dollars in damage.[5] Since

its previous invasion of Ukraine in 2014, Russia has continued to use Ukraine as a "playground" to field growing cyber weapons. Ukraine's historical Soviet infrastructure served well as a backdrop for understanding its grid structure and technological capabilities.

Russian President Vladimir Putin may have hoped for a quick rout of Ukraine's defenses, which would not warrant the destruction of civilian networks, the underlying goal being to not alienate Ukrainian citizens while still establishing a puppet regime in Kyiv. Russia may have foreseen the need to use Ukrainian telecommunication networks, likely for their own communication needs as well as intelligence-gathering and targeted information collection on Ukrainian forces. This may have led to a decision to not use more forceful cyber and electronic warfare in the early stages of the war.[6]

The evidence of attempted or successful cyberattacks will likely come out over time. Nearly nine of 10 cyberattacks worldwide target Russia or Ukraine, according to U.S. cybersecurity firm Imperva.[7] There may be a simpler answer once kinetic war is fully on the table and underway via land and air weapons such as missiles, tanks, and infantry; these hard tools are the instruments of choice versus the "gray zone" of cyber.[8] But such a calculation could change in the days and weeks ahead as Russia attempts to solidify and maintain gains while seeking leverage in negotiations. Logistical, morale, and tactical challenges combined with the difficult nature of urban combat and maintaining supply lines has impacted Russia's ability to advance on multiple axes.

Ukraine, in turn, has recruited a volunteer "IT Army," tasking a garden variety of hacktivists with DDoS attacks on Russian and Belarusian government, energy, and banking websites, including the identification and reporting of Russian disinformation campaigns.[9] Hackers such as the Belarusian Cyber Partisans have focused on wreaking havoc on Belarus' train system with attempts to slow down Russian troops and equipment. The decentralized hacking group Anonymous announced they were "officially in a cyber war against the Russian government" and has targeted Russian state-controlled television networks and attacked and intercepted Russian radio receivers.[10]

Russia has its own proxy and criminal-syndicate actors that have declared support and issued calls to arms for Putin's war. Conti, a well-known and prolific ransomware group, declared they would "strike back at the critical infrastructures of an enemy" who carried out actions against Russia. Since then, they suffered a massive data leak that included internal discussions, Bitcoin addresses, and details of past attacks.[11]

## Evolving Conflict: Danger Ahead

As the war continues to evolve, an assortment of concerns will shape not only the current battlefields in Ukraine, but also actions and behaviors around the globe.

**State-Sponsored, Non-State, and "Hacktivist" Cyber Actors.** This current conflict is a target-rich environment, and not just for those feeling the most significant impacts in Ukraine. Other prolific actors, such as China, Iran, and North Korea, may seek to take advantage of the "fog of war." Such actors are able to utilize a wide set of tools and capabilities in espionage and cyber-targeting of critical infrastructure, the military-industrial base, financial sectors, and policymakers. Attribution will be blurred and likely difficult to assess quickly.

State-based hackers in Belarus, China, and Russia are believed to be targeting Poland, Ukraine, and others in the European Union (EU).[12] Attacks have involved Russian military group "Fancy Bear" using "large credential phishing campaigns" to target a Ukrainian media company, Belarusian group "Ghostwriter" using phishing credentials and deploying MicroBackdoor malware against Polish and Ukrainian government and military actors, and China-based group "Mustang Panda" targeting European diplomatic entities.[13] Russian activities in the United States also continue. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued multiple recent warnings regarding Russian malicious cyber-activity and possible exploitations.[14] Recently, cyber law enforcement action from the Department of Justice and the FBI successfully removed Russian malware to create "botnets" from around the globe.[15]

Russia maintains a wide range of capabilities in cyberspace, including offensive and espionage operations. In recent years, the U.S. government has outlined previous instances of Russian state-sponsored actors breaking into "air-gapped" networks within supply-chain vendors of American power companies, in which they "could have thrown switches" according to Jonathan Homer, former chief of industrial-control-system analysis at the Department of Homeland Security (DHS).[16] They have also shown their ability to covertly maintain presence for long periods of time in government systems with the 2020 discovery of the SolarWinds vulnerability that compromised at least nine federal agencies, including DHS, and at least 100 private companies.[17]

The addition of geopolitically motivated "hacktivists" at scale, along with conventional nation-state cyber actors, could find themselves stepping across unknown "red lines" or activities that could bleed over to North Atlantic Treaty Organization (NATO) countries.

As Putin grows increasingly frustrated with U.S. and European Union (EU) economic and technological sanctions, along with western military equipment flowing into Ukraine, he may seek to use his historical cyber tools and strategy to lash out at European allies or on American soil. Brief cyber-ransomware incidents or degradation of information technology systems can cause, at minimum, consumer panic and fear in U.S. markets such as gasoline and food supplies. This was the case in the Colonial Pipeline and JBS meatpacking incidents last summer.[18] The Biden Administration continues to warn the private sector, especially critical infrastructure nodes such as energy and power, water, hospital, and financial-sector companies, of the risk and "evolving threat intelligence, that the Russian government is exploring options for potential cyberattacks."[19]

**Hack and Dump/Election Interference.** Another infamous tool in Putin's toolbox is his intelligence services ability to "hack and dump" collected information to cause political or economic turmoil on adversaries. Examples include Russian activities ahead of the 2016 election cycle with the hack of the Democratic National Committee as well as possible links to the leak of 9 gigabytes of French President Emmanuel Macron's campaign e-mails during the 2017 French elections.[20]

The issue of the Russian invasion of Ukraine scrambled the race in France's recent election. Russia could attempt nefarious activities dependent on Macron's and France's levels of support to Ukraine.[21] The United States' midterm elections this November will continue to serve as a glowing target for nefarious Russian activity (along with others such as China and Iran) based on recent elections.

For example, the FBI recently warned that election officials in nine U.S. states were targeted with sophisticated phishing attempts in October 2021. It likewise expects "cyber actors will likely continue or increase their targeting of US election officials with phishing campaigns in the lead-up to the 2022 midterm elections."[22]

**Space.** The cyber war is not limited to Earth. Space-based government and commercial satellites and assets are vital, and include ever-increasing technologies for communications, global positioning systems (GPS), imaging, and increasingly for broadband services.

Russia maintains a vast array of anti-satellite (ASAT) weaponry aimed at disrupting U.S. and allied nations' space capabilities. The 2022 Office of the Director of National Intelligence (ODNI) *Annual Threat Assessment* noted Russia is "developing, testing, and fielding an array of nondestructive and destructive counterspace weapons—including jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and

ground-based ASAT capabilities—to target US and allied satellites."[23] SpaceX Chief Executive Officer Elon Musk's moves recently to activate Starlink satellites for Ukraine coverage, as well as shipments of the necessary ground-based receivers, received significant attention.[24] Musk has acknowledged concerns that usage of the receivers could be triangulated by Russian forces to locate and target strikes, but it is unclear if this has occurred.

SpaceX has reportedly shifted resources to account for likely Russian jamming of Starlink satellites.[25] Musk said his company had "reprioritized to cyber defense & overcoming signal jamming"[26] and that some terminals near conflict zones had been seeing hours of Internet blocking while a software update provided by the company would assist in bypassing ongoing jamming attempts.[27]

U.S. communications company Viasat's KA-SAT broadband geostationary satellite has similarly seen disruptions due to cyberattacks, which has impacted coverage in Ukraine and European countries such as France and Germany. Over 5,800 European windmill turbines were reportedly offline due to service disruptions, turbines that collectively produce a total capacity of 11 gigawatts of energy.[28] According to recent Reuters reporting, Western intelligence agencies including the National Security Agency (NSA), French government cybersecurity organization (Agence Nationale de la Sécurité des Systèmes d'Information), and Ukrainian intelligence are assessing whether the remote sabotage of a satellite Internet provider's service was the work of Russian state-backed hackers preparing the battlefield by attempting to sever communications.

Viasat serves as a defense contractor for the United States, as well as other allies including Ukraine. According to Reuters' review of government contracts, KA-SAT has provided Internet coverage to Ukrainian military and police units.[29] Victor Zhora, Deputy Chairman of the State Service of Special Communications and Information Protection of Ukraine, said the disruption caused a "huge loss in communications in the very beginning of the war."[30] Viasat recently provided a known overview calling it a "multifaceted and deliberate cyber-attack" that impacted "several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe."[31]

## Defend Forward

According to recent reports, "cybermission teams" from U.S. Cyber Command have been active in Eastern Europe ahead of the conflict, assisting

Ukrainians' cyber defenses and infrastructure resiliency in preparation of expected Russian cyberattacks.[32] NSA Director and U.S. Cyber Command Head General Paul Nakasone testified recently at the Senate Intelligence Committee's Annual Threat Assessment hearing that the role of the U.S. and its allies in recent years to shore up areas of Ukraine's cybersecurity challenges had made an impact in the early days of the war: "We've worked very, very hard with Ukraine over the past several years, really since the shut down of energy in 2015. We had hunt forward teams from U.S. Cyber Command in Kiev, we worked very, very closely with a series of partners at NSA and the private sector to be able to provide that information."[33] That success is difficult to publicly grade in the near term, but the likelihood is that battles in cyber and space have just begun.

Cyber policy in recent years has seen a variety of changes to streamline decision-making and the speed at which Cyber Command can more quickly take proactive action.[34] Changes during the Trump Administration, such as the replacement of Presidential Policy Directive (PPD-20) with National Security Presidential Memorandum (NSPM)-13, established a process to delegate authorities to operating agencies, including to the Department of Defense, to conduct "time-sensitive military operations in cyberspace."[35]

Recent reports that the Biden Administration has initiated an "inter-agency review process" to scale back these changes to cyber authorities are concerning.[36] Restoring the Obama Administration's paralysis-by-analysis would lead back to siloed infighting among competing agencies and slow, persistent, defend-forward types of actions. Establishing deterrence below the threshold of an armed conflict is an important tool that should be maintained with other conventional, diplomatic sanctions and law enforcement and prosecutorial efforts.[37]

In March 2022, NATO unanimously took the important step to admit Ukraine to the highly capable, Estonian-based Cooperative Cyber Defence Centre of Excellence (CCDCOE).[38] This action should have occurred prior to the Russian invasion, but it is a welcome move that can immediately assist Ukraine now and in the future.

## Russian Censorship, Suppression, and Disinformation in the Age of Digital Authoritarianism

In the past few years, the world has seen an explosion of digital surveillance and censorship technologies. Regimes such as Afghanistan, China, Cuba, Iran, Russia, and Venezuela have demonstrated the ability and willingness to utilize these tools.

**Censorship and Suppression.** As the Internet and associated telecommunication technologies have further emerged and become the primary global communication conduits, autocratic regimes' "digital authoritarianism" playbook has been to surveil and censor their citizens with an aim to extend and consolidate their existing power structures. China has proliferated the development and use of censorship technologies to support regimes facing challenges—most recently in Venezuela and Cuba, the latter quelling 2021 protests with the help of Chinese telecommunications providers Huawei and ZTE.[39]

President Vladimir Putin and Russian crackdowns are a primary example. In recent weeks, Russia has moved forward with substantial censorship restrictions—new laws passed in a matter of days further curbing freedom of expression, throttling and shutting down multiple social media networks, including Facebook, Instagram, and Twitter.[40] Russia continues to ramp up campaigns to censor and spin the Ukrainian invasion on more popular platforms such as U.K.-based Telegram, U.S.-based YouTube, and China-based TikTok—the latter cutting off access to most overseas accounts and restricting the description of the war in Ukraine as anything other than a "special military operation."[41]

Large-scale interment and arrests of protestors of the war—more than 13,000 in the first two weeks according to a Russian human rights group—will likely continue in the near future.[42] The significant suppression of independent and uncensored media in Russia leaves Putin's narratives of the "operation" unchallenged.

**Pushback.** Nonetheless, there are those attempting to fight back. For the first time since 1991, the British Broadcasting Corporation (BBC) News activated its shortwave radio programming for four hours a day in English, broadcast to audiences in western Russia as well as Ukraine. Russian Internet regulator Roskomnadzor restricted access to the BBC's website as a cat-and-mouse game emerges to relay the truth to the Russian people.[43]

The United States has historically funded circumvention tools and advances in technology to combat such trends through the U.S. Agency for Global Media and, specifically, the Open Technology Fund (OTF). The OTF "funds internet freedom technologies at every stage of the development cycle from proof-of-concept to on-the-ground deployments to multi-year efforts" via direct funds, labs, fellowships, network support, and rapid response.[44]

Digital authoritarianism has spread more quickly than the capacity of current technologies to keep pace with adversaries to free speech and independent information. Virtual private network (VPN) circumvention

tools such as Psiphon or anonymizing browser Tor have seen explosions in downloads and usage to channel information past Russia's censorship blockades. Similar bursts in the use of such platforms occurred during protests in Cuba in the summer of 2021 and Belarusian protests after President Alexander Lukashenko's fraudulent election.

**Deepfakes.** Other technological threats are on the horizon. In recent years, the FBI has warned of ongoing foreign adversary development of "deepfakes" and the use of synthetic content in influence campaigns, spear phishing, and social engineering.[45] A poorly doctored deepfake, presumably Russian-made, of Ukrainian President Volodymyr Zelensky calling on Ukrainians to surrender circulated recently and was eventually removed from social media platforms after it was identified. Zelensky and Ukraine's Center for Strategic Communication had already warned Ukrainian citizens to expect deepfakes such as this ahead of the video's release.[46]

Although the warning was a relative success case in this instance, deepfakes and ever-increasing technological abilities by U.S. adversaries to create such content, along with technical difficulties in quickly identifying such disinformation, serves as a warning. Content can circulate quickly in today's social media environment, and, identified quickly as fake or not, leaves a presumption of proof needed on what is real and what is not.

These crackdowns are not abating, however. As countries such as China and Russia seek to spread further use of technologies and capabilities to those who favor the use of disinformation and censorship as bulwarks to their power, additional technological tools from the U.S. and its allies to protect privacy and communication—and to counter these measures—will be necessary.

**The INFO Act.** The U.S. Congress recently passed Ukrainian supplemental aid that included funding for combatting informational warfare in Russia and Ukraine and maintaining communication links for independent information.[47] In addition, recently introduced legislation from Senators John Cornyn (R–TX) and Amy Klobuchar (D–MN) "would authorize the U.S. State Department and Department of Defense to enter into contracts with satellite cellular and internet providers to provide direct connectivity in conflict regions." Senate Foreign Relations Committee Chairman Robert Menendez (D–NJ) and Senator Marsha Blackburn (R–TN) introduced a measure, the Internet Freedom and Operations (INFO) Act of 2022, that would further authorize resources for various Internet freedom programs through the Department of State and the U.S. Agency for International Development. Importantly, the legislation would dedicate resources to Internet freedom and circumvention technologies through the Open Technology Fund with expedited authorities in crises situations such as now.[48]

As mentioned earlier, Internet broadband coverage via satellite, such as SpaceX's Starlink, could provide additional communication and Internet links for those in Ukraine—with some caveats.[49] These technological solutions become more difficult in areas where ground-based receivers needed for satellite Internet coverage are unable or difficult to place due to supply-line issues in Ukraine or in countries such as China, Cuba, Iran, and North Korea. Support for "old-school" communications mechanisms, such as radio and access to broadcast mediums such as Radio Free Europe/Radio Liberty broadcast from outside Russia and Ukraine, will remain essential.

**Research and Development Efforts.** Finally, important research and development efforts are underway at agencies such as the Defense Advanced Research Project Agency (DARPA) and the Intelligence Advanced Research Project Agency (IARPA).[50] Digital authoritarianism presents immense challenges for the U.S. national security apparatus. This includes ubiquitous technical surveillance, including pervasive surveillance cameras, biometrics, facial recognition, data collection from uses of one's smartphone to one's vehicle, and new uses of artificial intelligence of data sets to analyze civilians and national security personnel.[51]

Dr. Joshua Baron, a program manager at DARPA, outlined the need for a government-wide effort to establish a "formal, rigorous framework to reason about large-scale surveillance and censorship." Understanding how an adversary such as China could exploit surveillance and censorship is essential. This includes the development of technology, software, and algorithms "to enable repressed populations to use information technology (particularly Internet-based systems) even if the adversary controls various components of that technology (e.g., mobile devices, Internet architecture components). Baron additionally noted research areas to understand and counter Artificial Intelligence–enabled surveillance and "rapid counter-censorship messaging algorithms and software that discovers adversary-censored topics and modifies desired messages to remain uncensored, disrupting adversary censorship efforts."[52]

The U.S. has recently begun making steps in this direction. For example, the Office of the Director of National Intelligence's Science and Technology Investment Guidance for fiscal years 2022–2026 seeks to track technologies research to long-term, over-the-horizon threats while breaking down barriers and connecting program managers with private-sector industry and technology developers. Importantly, the strategy, if implemented properly and efficiently, is to "catalyze investments" as the U.S. works to stay at the cutting edge of emerging and advanced technologies.[53]

These efforts will require partnerships among U.S. national security community members, broader communication and technology efforts, and private-sector willingness and resources to counter the technological aspirations of countries such as China and Russia.

## Intelligence-Sharing

U.S. and NATO allies have been assisting Ukraine since the 2014 Russian invasion in order to modernize and train its military, gather and share intelligence, and secure communications and improve cybersecurity. A plethora of U.S. intelligence, surveillance, and reconnaissance aircraft such as the E-8C, RC-135V/W Rivet Joints, U-2S, and the RQ-4 Global Hawk became indispensable intelligence-gathering collectors.[54] Once Russian forces began striking Ukraine again in late February 2022, the United States pulled back these ISR aircraft and unmanned aerial systems that had gathered intelligence of the Russian military buildup along Ukraine's borders: They were then forced to peer over Ukraine from NATO territories.[55]

Intelligence-sharing and its timeliness and specificity became a vocal outcry from lawmakers in the early weeks of the conflict.[56] Senator Ben Sasse (R–NE) noted: "We are sending them intelligence. But we have lawyers delaying the process at way, way too many steps. And we shouldn't be letting technicalities get in the way of helping the Ukrainians fight back."[57] Recent reporting indicates that the White House "modified existing guidance" for the Pentagon and Intelligence Community (IC). According to *The Wall Street Journal*, the Administration and the Pentagon have worked to move classified information via secure communications equipment to assist the Ukrainian military quickly with "detailed, tactical data on Russian troop movements."[58]

The U.S.–Ukraine intelligence relationship has evolved and grown significantly closer since 2014.[59] Western intelligence officials have historically noted concerns that Russian intelligence likely infiltrated various elements of the Ukrainian military, government, and intelligence apparatuses. Senate Select Committee on Intelligence Chairman Mark Warner (D–VA) said recently, "We also have to realize, unfortunately, many of the Ukrainian services have been penetrated by the Russians over many years, so we have to protect our sources and methods."[60] Due to this, the necessity of "scrubbing" or "downgrading" classified material is needed to properly secure transmittal and alleviate these counterintelligence concerns and protect sources. This must be done as expeditiously as possible, though.

Commercial and open-source intelligence have grown immensely with technological development and ballooning data creation in recent years. The Intelligence Community and lawmakers have advocated for better use of this information for well over two decades, yet there are still many gaps to creating an environment in which analysts and intelligence customers can maximize its usage. Emily Harding of the Center for Strategic and International Studies proposed a novel idea of an Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community (OSCAR) to remedy the cultural, security, and policy problems that have stymied the IC from expanding the use of cloud, artificial intelligence/machine learning, and open-source intelligence.[61] Avoiding the trap of importing vast amounts of unclassified open-source data into the classified cloud structures of the IC is key. Commercial, scalable cloud capabilities offer a vast consortium of tools that analysts could use in an unclassified environment to further shape classified analysis. The IC, however, needs to do a far better job of establishing a rules-based approach (known as tradecraft) for integrating open-source information into the analysis that is delivered to decision-makers. Open-source social media (such as Telegram) and commercial satellite imagery from firms such as Maxar Technologies openly discussed and showed Russian military buildups ahead of the invasion, with the further support of downgraded and declassified information from the IC.

With advanced capabilities of commercial satellite and imaging vendors playing a role in intelligence-gathering and publicizing information, important questions remain for policymakers on response scenarios. Christian Davenport of *The Washington Post* recently asked:

> What happens if a commercial entity from the United States provides actionable intelligence—images of a Russian convoy, for example—to a foreign government that then uses that data to mount an attack? Would Russia be justified in attacking the satellite? And if that were to happen, how should the U.S. government respond?[62]

## Recommendations

The U.S., NATO, and the EU must remain on high alert in their monitoring of Russian cyber, space, and intelligence movements—as well as be prepared for outside proxies, on either side of the ledger, that could cause possible collateral damage. The "Shields Up" mantra to U.S. critical infrastructure and businesses is welcome, but everyday Americans must also be

prepared for a conflict that could spill into their backyard at any moment. Below are some key near-term recommendations.

The Administration should:

- **Expedite Cyber-Breach Notification Rulemaking—and Ensure It Does Not Become a Red-Tape Paper Exercise.** Congress recently passed cyber-breach notification requirements that leaves up to 24 months for CISA to publish a notice of proposed rulemaking for the program.[63] With varying industries and definition decisions left out of the law, such as what constitutes a "significant" incident, Congress will rely on CISA to flush out the terms of the program. The government and private sector should expedite this period as much as possible considering the delays in passage of the legislation and the cyber threat picture that continues to emerge. A much greater sense of urgency is required.

- **Ensure Final Rulemaking Includes Expedited Information-Sharing with the Private Sector and Law Enforcement, as Needed.** CISA, the Department of Justice, and the Federal Bureau of Investigation remained at odds on the final legislation due to conflicts about who received the breach notifications initially and the liability protections it provided. The FBI remains a potent and necessary piece of the cybersecurity puzzle as it maintains cyber investigative capabilities and authorities, as well as local and regional relationships in the 56 field offices and roughly 350 resident agencies around the U.S. Congress. The Administration should be clear-eyed that those cyber responsibilities will remain a team exercise in which speed in response and clear lanes of control will be necessary.

  The liability shield for reporting to CISA contained in the final cyber-breach notification bill should extend to the FBI. FBI Director Christopher Wray, in a recent hearing, said many field agents respond within an hour to an incident and "businesses that come forward like that, when they talk to the agents out in the field, [should] have protection from liability for doing so, and not just reporting through some longer term means to some bureaucracy somewhere in DC."[64] Carrots and sticks matter when government regulation is involved, but the critical infrastructure that is privately owned must see the interlocutor relationship and information gleamed from it positively for these programs to be a success.

- **Tread Lightly and Carefully When Considering Future Critical Infrastructure Cyber Regulations.** The Administration has proceeded with and signaled to various critical infrastructure nodes the desire to regulate cybersecurity structures. The Transportation Security Administration (TSA) proceeded to further regulate the pipeline industry after the Colonial Pipeline ransomware attack in 2021. According to oil and gas pipeline operators, the regulations are "full of unwieldy or baffling requirements that could actually jeopardize pipeline safety and fuel supplies." Robert M. Lee of the cybersecurity firm Dragos stated, "In every sense, TSA has screwed this up."[65]

  With different regulatory agencies overseeing areas of critical infrastructure, including the oil and gas industry, health care and hospitals, banking and financial sectors, and electric and grid reliability, one-size-fits-all solutions will not work and must include expertise when promulgating any new regulatory requirements. At the same time, industry officials who have treated the cybersecurity of their operating systems and information technology systems as an afterthought must expeditiously provide further resources and improvements to their architecture.

- **Expedite Improvements in Public–Private Sector Engagements, Including Additional Cyber Exercises and Critical Infrastructure Research and Development.** The recent creations of CISA's Joint Cyber Defense Collaborative and NSA's Cybersecurity Collaboration Center are welcome and needed. Exercises such as the recently completed Cyber Storm VIII should continue and add additional collaborators to prepare resilience and remediation scenarios.[66] In addition, research and development programs such as DARPA's Rapid Attack Detection, Isolation and Characterization Systems program to develop tools and technologies for "black start" recoveries during a cyberattack on the power grid should continue and grow, in addition to other projects at Plum Island, New York.[67]

  Additional areas of collaboration for research and private-sector engagement (in addition to the power grid and utilities) should further include elements of the finance and banking sectors. Recent successes have been seen with stronger public–private sector collaboration. This includes Microsoft's moves—within three hours—to update its virus detection systems after discovering malicious malware named

FoxBlade impacting Ukraine and working with the Administration to share information quickly with other EU states that could be impacted.[68]

- **Concentrate Attention Toward Opportunity-Seeking Nation-State Adversaries Such as China, Iran, and North Korea.** Since the launch of the Russian invasion into Ukraine, the U.S. has seen Iran launch rocket attacks on U.S. installations in northern Iraq, North Korea testing a new intercontinental ballistic missile system, and China expressing openness to Russian requests for military and financial aid.[69] In an environment in which attribution of cyberattacks is difficult enough, adversaries that have common attributes and links to criminal cyber actors or personnel who serve in a moonlighting role may find themselves crossing unanticipated boundaries. As was seen in the aftermath of the Afghanistan withdrawal debacle, America's adversaries will continue to test the resolve and dedication of the U.S. on the international stage. This includes likely provocations in their individual areas of responsibility: U.S. deterrence and strength will be key.

States and the Administration should:

- **Focus Cybersecurity Efforts on Improving Resilience and Shared Lines of Effort.** Cybersecurity in recent years has evolved into a series of reciprocating headlines. Ransomware, espionage, and cyber actions that have escalated toward sections of critical infrastructure have focused lawmakers and the Biden and Trump Administrations on fixing the government's cyber structure and policies. A silver bullet solution from Washington, DC, via a federal agency such as CISA or a National Cyber Director will not reduce the threat picture to zero, nor can such agencies respond to every crisis around the country. Although recent hiring policy changes could improve onboarding retention efforts, CISA and many other cyber-related agencies have thousands of open cyber- and technological-related billets.

  Recent NDAAs and legislative efforts have made moves toward clarifying the role and payment structure of the National Guard in various response scenarios including ransomware and additional regional training.[70] Geographically disbursing cyber-capable personnel for emergencies via the National Guard, with the parallel ability to maintain more lucrative jobs in the private sector, would provide

an additional arsenal for governors and localities to assist in various cyber incidents.[71] Just as the Stafford Act[72] has become abused by states as a get-out-of-jail-free card in less severe emergencies (overstretching the Federal Emergency Management Agency), any policy structure implemented by the Department of Defense alongside the National Guard must account for proper resources being available and maintained by states.

Congress, the Department of Defense (DOD), and states should move expediently to implement recommendations and any legal framework changes within recent National Defense Authorization Act–required reports on clarifying Titles 32 and 10, and State Active Duty activities such as dual-status command, funding ratios, and technical training assistance.[73] As of summer 2021, governors had activated their National Guards at least 41 times to respond to cybersecurity-related matters of state and local governments.[74]

- **States Should Expedite the Building and Maintenance of Specific Cyber Resources, Workforce Capabilities and Training, Exercise-Response Scenarios, and Consider Memoranda of Understanding with Nearby States for Information-Sharing and Best Practices.** In addition to exercises such as CISA-hosted "Cyber Storm," states should develop their own state, local, and private-sector exercises with partners to establish resiliency and remediation plans. Many states have made large strides in improving their cybersecurity architectures and response plans in recent years, but these need to be expedited and remain a priority for every governor and state legislature in the country.

  Only 23 states currently maintain state defense forces or guards, with the most recent addition coming from Florida's revival of their historic guard.[75] All states should provide and budget for a state defense force or, in conjunction with nearby states, establish specific cyber-defense capabilities that can be called upon in emergencies. From critical infrastructure to election systems, adversaries such as China, Iran, and Russia will continue to probe weaknesses and opportunities. States should look to North Dakota as an example of leadership in the development of an interstate cybersecurity operations center (along with nearby states) for the purposes of information-sharing and collaboration.[76] States such as Florida, where Governor Ron DeSantis

has prioritized resources for cybersecurity and information-technology workforce opportunities and education prioritization in grades K–12, higher education, and apprenticeship opportunities, will be much needed elsewhere as critical gaps remain in capable workforces in these fields.[77]

The Administration and Congress should:

- **Expand Bilateral Cooperation with Strategic Allies, Including Further Development of U.S. Cyber Command, NSA, U.S. Space Force, and NATO Cyber Assets and Authorities.** The United States, the United Kingdom, and advanced NATO cyber partners such as Estonia and Romania remain at the front lines of cyber offense and defense. Further evaluations of the effectiveness, resourcing, and future structuring of these teams within the current conflict, as well as actions taken in the 2018 and 2020 election cycles, will be vital to maintaining and improving an important capability for the U.S.[78] The National Security Council should retain the Trump Administration's approach and drive operating agencies to establish deterrence below the threshold of an armed conflict. Further improvements can be made in interagency communication and coordination on offensive cyber actions, but reversals back to the Obama Administration's siloed and bureaucratic approaches are unwarranted.

  In addition, the U.S. should further strengthen diplomatic and military-to-military engagements on cyber cooperation and training with the Estonian-based CCDCOE and the newly established European Union Cybersecurity Industrial, Technology and Research Competence Centre based in Romania. Bilateral cybersecurity cooperation efforts should be further expanded upon with countries such as India, Japan, South Korea, and Taiwan, as the U.S. examines the ever-growing Chinese cyber threat. Proper funding, resources, and expertise should be expanded upon for the development of space cybersecurity technologies, including substantial collaboration and information-sharing with the private and commercial space sectors.

- **Increase Attention and Resources on the Operational Technology (OT) Cybersecurity of Commercial and Military Platforms.** Nation-state threats continue to grow as informational technology nodes intertwine with OT platforms. Commercial critical

infrastructure and transportation systems, such as energy production and pipelines, water and waste management, airlines, and passenger and freight rail, all rely heavily on operational technology platforms.[79] Defense weapons systems will also face a multitude of challenges from potential cyberattacks and electronic warfare. Adversaries such as China have sought through cyber espionage to intrude into the U.S. defense industrial base to understand U.S. capabilities.[80] Nearly a decade ago, a report by the Department of Defense's Defense Science Board provided a list of U.S. weapons systems that were at least partially compromised by Chinese hackers.[81] Sections 1505 and 1528 of the fiscal year 2022 National Defense Authorization Act contained several directives to the Department of Defense for improvements, zero-trust architecture, and accountability in OT cybersecurity.[82] These provisions should be expediently funded and implemented.

- **Increase Support of Internet Freedom Programs that Promote Anti-Censorship Technologies and Circumvention Tools.** Congress has historically supported the research and development of anti-censorship technologies to promote communication and information-sharing in autocratic-regime-controlled areas around the world such as China, Cuba, Iran, Russia, and Venezuela. As countries such as China proliferate surveillance and censorship technologies to like-minded regimes, it behooves the United States to take a leadership role in supporting and encouraging the development of privacy-preserving and censorship circumvention technologies to assist in proliferating independent information to citizens behind autocratic lines. Additionally, further research and recommendations should be considered as they relate to technological capabilities to detect deepfakes, and streamlined interagency measures are needed rapidly disseminate that information within the government and with private-sector partners.

- **Review, Streamline, and Improve Intelligence-Gathering and Sharing with Ukrainian Military, Security Services, and Allied Partners.** Although recent concerns on expedient intelligence-sharing have been assuaged, the Biden Administration, the Department of Defense, and Intelligence Community should continue to look for areas that could be further improved and expedited. Concerns related to the proper protection of sources and methods and the secure communication of information are valid, but the U.S. should err on the

side of taking measured risks. These include assisting the Ukrainian government with connections to U.S. commercial and open-source companies such as satellite imaging companies with whom they could contract.

Policymakers should also clarify response scenarios and responsibilities of U.S. and allied commercial space assets being targeted by adversaries. In the longer term, intelligence agencies should look to quickly downgrade and release intelligence information related to Russian (or others, e.g., Chinese or Iranian) efforts to engage maliciously in the U.S. midterms or allies' elections, such as the recent French elections.

- **Review and Expedite the Use of Commercial and Open-Source Intelligence (OSINT).** The Intelligence Community and Congress have been making note of the increased need and use of open-source and commercial intelligence. The IC needs to treat OSINT as an intelligence discipline that is provided as a service of common concern among the 18 IC elements. Technological advances and cost reductions in commercial space satellites, for example, could be game changers that could offer redundancy, resilience, and increased capabilities alongside classified national security assets.[83] Scaling the use of open-source intelligence has been called for ad nauseum by lawmakers and leaders in the Intelligence Community for well over two decades. The IC needs to establish tradecraft rules that clarify how open-source information is used in analytic products. Congress need not add additional reporting requirements to the IC and the DOD's queue on developing a plan for OSINT: It is time for action and oversight accountability from Congress.

- **Conduct Periodic Interagency Reviews of Ongoing Hybrid Actions, Capabilities, and Threats.** Understanding the existing environment, including what has worked well and what has worked poorly, followed by actionable lessons learned that can be rapidly deployed, as well as understanding future resources needed, are key. No longer can the Administration and Congress seek additional multi-year reports and reviews to fix well-known problems. Leaders within the executive branch with proper oversight by authorizing committees must move with haste from technological improvements to breaking down long-standing bureaucratic barriers.

These recommendations are by no means exhaustive. It is important that all stakeholders act with speed and due diligence as each passing day in Ukraine creates long-term ramifications that will reverberate around the globe.

## Conclusion

War is, by nature, an awful affair. How this war ends no one knows, but the United States and our allies can make a difference in the days ahead as we look at a future with hybrid conflict changing the paradigm. The actions currently being taken by Vladimir Putin and the Russian military through missiles, tanks, and infantry are putting countless innocent Ukrainian citizens in harm's way.

As the United States and our allies go forward, the importance of cybersecurity, intelligence-sharing, technological innovation, and access and understanding of independent media and information are more important than ever. Nation-states such as China, Iran, North Korea, Russia, and others will continue to use these mediums to punch above their weight and attempt to supplant the United States. The shadow wars happening may not have matched the "movie-like" expectations of many, but this by no means negates their constant and persistent threats.

**Dustin Carmack** is Research Fellow for Cybersecurity, Intelligence, and Emerging Technologies in the Border Security and Immigration Center at The Heritage Foundation.

## Endnotes

1. Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ (accessed March 17, 2022).
2. Andrew E. Kramer, "Hackers Bring Down Government Sites in Ukraine," *The New York Times*, January 14, 2022, https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html (accessed March 2, 2022), and Microsoft Threat Intelligence Center (MSTIC), "Destructive Malware Targeting Ukrainian Organizations," January 15, 2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (accessed March 2, 2022).
3. Steve Holland and James Pearson, "U.S., U.K.: Russia Responsible for Cyberattack Against Ukrainian Banks," Reuters, February 18, 2022, https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/ (accessed March 2, 2022); Dustin Volz, "Malware Detected in Ukraine as Invasion Threat Looms," *The Wall Street Journal*, February 23, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo (accessed March 2, 2022); "HermeticWiper: New Data-Wiping Malware Hits Ukraine," ESET, February 24, 2022, https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/ (accessed March 2, 2022), and A.J. Vicens, "Top Ukrainian Cyber Official Praises Volunteer Hacks on Russian Targets, Offers Updates," CyberScoop, March 15, 2022, https://www.cyberscoop.com/it-army-ukraine-caddywiper-viasat/ (accessed March 16, 2022).
4. Sean Lyngaas, "Russian Military-Linked Hackers Target Ukrainian Power Company, Investigators Say," CNN, April 14, 2022, https://www.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html (accessed April 20, 2022).
5. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed March 17, 2022).
6. Jason Healey, "Preventing Cyber Escalation in Ukraine and After," *War on the Rocks*, March 9, 2022, https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/ (accessed March 9, 2022).
7. Frank Konkel, "More than 80 Percent of Cyberattacks Worldwide Happening in Russia or Ukraine," Nextgov, March 10, 2022, https://www.nextgov.com/cybersecurity/2022/03/more-80-cyberattacks-worldwide-happening-russia-or-ukraine/362964/ (accessed March 11, 2022).
8. Ciaran Martin, "Cyber Realism in a Time of War," Lawfare Blog, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war (accessed March 3, 2022).
9. Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, February 27, 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/ (accessed March 3, 2022).
10. Monica Buchanan Pitrelli, "Anonymous Declared a 'Cyber War' Against Russia. Here Are the Results," CNBC, March 16, 2022, https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html (accessed March 16, 2022).
11. Brian Krebs, "Conti Ransomware Group Diaries, Part I: Evasion," Krebs On Security, March 1, 2022, https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/ (accessed March 11, 2022).
12. Shane Huntley, "An Update on the Threat Landscape," Google Threat Analysis Group (TAG), March 7, 2022, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ (accessed March 11, 2022).
13. A.J. Vicens, "Against Backdrop of Russian–Ukraine War, Researchers Witness Flurry of Nation-Aligned Hacking," CyberScoop, March 8, 2022, https://www.cyberscoop.com/russia-belarus-china-poland-hack-europe-nato/ (accessed March 11, 2022).
14. Cybersecurity and Infrastructure Security Agency, "Russia Cyber Threat Overview and Advisories," https://www.cisa.gov/uscert/russia (accessed April 6, 2022).
15. Kate Conger and David E. Sanger, "U.S. Says It Secretly Removed Malware Worldwide, Pre-Empting Russian Cyberattacks," *The New York Times*, April 6, 2022, https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html (accessed April 7, 2022).
16. Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *The Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (accessed March 17, 2022).
17. Robert McMillan and Dustin Volz, "SolarWinds Hackers Continue to Hit Technology Companies, Says Microsoft," *The Wall Street Journal*, October 25, 2021, https://www.wsj.com/articles/microsoft-solarwinds-hackers-continue-to-hit-technology-companies-11635145200 (accessed March 17, 2022).
18. Clifford Krauss, Niraj Chokshi, and David E. Sanger, "Gas Pipeline Hack Leads to Panic Buying in the Southeast," *The New York Times*, May 12, 2021, https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html?smid=url-share (accessed March 11, 2022)
19. Tonya Riley, "White House Issues Call to Action in Light of New Intelligence on Russian Cyberthreat," CyberScoop, March 21, 2022, https://www.cyberscoop.com/russia-ukraine-white-house-hack/ (accessed March 21, 2022).
20. Jean-Baptiste Jeangène Vilmer, *The "Macron Leaks" Operation: A Post-Mortem*, The Atlantic Council and L'Institut de Recherche Stratégique de l'École Militaire, June 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed March 11, 2022).

21. Benjamin Dodman, "Ukraine War Puts France's NATO-Sceptic Presidential Candidates in a Tight Spot," France24, March 4, 2022, https://www.france24.com/en/france/20220304-ukraine-war-puts-france-s-nato-sceptic-presidential-candidates-in-a-tight-spot (accessed March 11, 2022).
22. Federal Bureau of Investigation, "Cyber Actors Target U.S. Election Officials With Invoice-Themed Phishing Campaign to Harvest Credentials," Cyber Division, March 29, 2022, https://www.ic3.gov/Media/News/2022/220329.pdf (accessed March 30, 2022).
23. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community, 2022*, February 2022, pp. 12–13, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (accessed March 14, 2022).
24. Morgan Meaker, "High Above Ukraine, Satellites Get Embroiled in the War," *Wired*, March 4, 2022, https://www.wired.com/story/ukraine-russia-satellites/ (accessed March 14, 2022).
25. Jeff Foust and Brian Berger, "SpaceX Shifts Resources to Cybersecurity to Address Starlink Jamming," SpaceNews, March 5, 2022, https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/ (accessed March 14, 2022).
26. Elon Musk, Twitter Post, March 4, 2022, 11:59 p.m., https://twitter.com/elonmusk/status/1499972826828259328?s=20&t=5UAZlm9p_TdCX1zH32sk4A (accessed April 6, 2022).
27. Elon Musk, Twitter Post, March 5, 2022, 3:32 a.m., https://twitter.com/elonmusk/status/1500026380704178178?s=20&t=1oYLo64P3IZxGpOalbL_jA (accessed April 6, 2022).
28. Joseph Henry, "Europe Cyberattack Results to 'Massive' Internet Outage: About 5,800 Wind Turbines Went Offline," Tech Times, March 5, 2022, https://www.techtimes.com/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm (accessed March 14, 2022).
29. James Pearson et al., "Exclusive: U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say," Reuters, March 11, 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/ (accessed March 14, 2022).
30. Vicens, "Top Ukrainian Cyber Official Praises Volunteer Hacks."
31. Viasat Corporate, "KA–SAT Network Cyber Attack Overview," Viasat, March 30, 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (accessed March 30, 2022).
32. David E. Sanger et al., "Arming Ukraine: 17,000 Anti-Tank Weapons in 6 Days and a Clandestine Cybercorps," *The New York Times*, March 6, 2022, https://www.nytimes.com/2022/03/06/us/politics/us-ukraine-weapons.html?smid=url-share (accessed March 14, 2022).
33. Maggie Miller, "Nakasone Credits U.S. Efforts With Preventing Major Russian Cyberattacks on Ukraine," *PoliticoPro*, March 10, 2022, https://subscriber.politicopro.com/article/2022/03/nakasone-credits-us-efforts-with-preventing-major-russian-cyberattacks-on-ukraine-00016234 (accessed March 14, 2022).
34. Dustin Carmack and Michael Ellis, "For Cybersecurity, the Best Defense Is a Good Offense," Heritage Foundation *Backgrounder* No. 3670, November 10, 2021, https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense.
35. Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ (accessed March 31, 2022).
36. Suzanne Smalley, "Biden Administration Is Studying Whether to Scale Back Trump-Era Cyber Authorities at DOD," CyberScoop, March 31, 2022, https://www.cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/ (accessed April 1, 2022).
37. Ibid.
38. Suzanne Smalley, "Ukraine, Looking to Fortify Itself Against Russian Attacks, Admitted to NATO Cyber Center," CyberScoop, March 4, 2022, https://www.cyberscoop.com/ukraine-admitted-nato-ccdcoe/ (accessed March 14, 2022).
39. Ken Dilanian, Joel Seidman, and Gabriel Sanchez, "A Project in El Salvador Shows How China Is Exerting Growing Power in America's Backyard," NBC News, September 4, 2021, https://www.nbcnews.com/politics/national-security/project-el-salvador-shows-how-china-exerting-growing-power-america-n1278464 (accessed March 17, 2022).
40. Anton Troianovski, "Russia Takes Censorship to New Extremes, Stifling War Coverage," *The New York Times*, March 4, 2022, https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html (accessed March 15, 2022).
41. Liza Len and Evan Gershkovich, "TikTok's Pullback in Russia Leaves More Space for Pro-Kremlin Propaganda," *The Wall Street Journal*, March 15, 2022, https://www.wsj.com/articles/tiktoks-pullback-in-russia-leaves-more-space-for-pro-kremlin-propaganda-11647370257 (accessed March 15, 2022).
42. John Goodwin, "Protesters in Russia Risk Arrest to Speak Out Against Putin's War," CBS, March 13, 2022, https://www.cbsnews.com/news/protesters-in-russia-risk-arrest-to-speak-out-against-putins-war/ (accessed March 15, 2022).
43. Sian Cain, "BBC Website Blocked in Russia as Shortwave Radio Brought Back to Cover Ukraine War," *The Guardian*, March 3, 2022, https://www.theguardian.com/media/2022/mar/04/bbc-website-blocked-in-russia-as-shortwave-radio-brought-back-to-cover-ukraine-war (accessed March 15, 2022).

44. U.S. Agency for Global Media, "Open Technology Fund," https://www.opentech.fund/ (accessed March 15, 2022). The FBI defines synthetic content as the "broad spectrum of generated or manipulated digital content, which includes images, video, audio, and text." Federal Bureau of Investigation, "Private Industry Notification," March 10, 2021, https://www.ic3.gov/Media/News/2021/210310-2.pdf (accessed April 7, 2022). The National Counterintelligence and Security Center defines spear phishing as "an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate…and targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents." Director of National Intelligence, " Spear Phishing and Common Cyber Attacks," https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf (accessed April 7, 2022). The FBI defines social engineering as "the use of deception, through manipulation of human behavior, to target and manipulate you into divulging confidential or personal information and using it for fraudulent purposes…psychologically manipulating people to take action to inadvertently give adversaries access to protected information or assets. Social engineering can also be used to embarrass and humiliate campaigns, voter groups, and others." Federal Bureau of Investigation, "Protected Voices: Social Engineering," https://www.fbi.gov/video-repository/protected-voices-social-engineering-083018.mp4/view#:~:text=Social%20engineering%20is%20the%20use,using%20it%20for%20fraudulent%20purposes (accessed April 7, 2022).
45. Shannon Vavra, "FBI Alert Warns of Russian, Chinese Use of Deepfake Content," CyberScoop, March 10, 2021, https://www.cyberscoop.com/fbi-foreign-actors-deepfakes-cyber-influence-operations/ (accessed March 21, 2022).
46. Suzanne Smalley, "Zelensky Deepfake Crude, But Still Might Be a Harbinger of Dangers Ahead," March 18, 2022, https://www.cyberscoop.com/zelenskyy-deepfake-troubles-experts/ (accessed March 21, 2022).
47. U.S. House of Representatives, "Ukraine Supplemental Appropriations Act, 2022," Appropriations Committee, March 2022, https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/Ukraine%20Supplemental%20Summary.pdf (accessed March 14, 2022).
48. Office of Marsha Blackburn, "As Putin Cracks Down On Free Press, Senators Blackburn, Menendez Unveil Bipartisan Legislation To Expand Internet Freedom," March 4, 2022, https://www.blackburn.senate.gov/2022/3/as-putin-cracks-down-on-free-press-senators-blackburn-menendez-unveil-bipartisan-legislation-to-expand-internet-freedom (accessed March 15, 2022).
49. Marina Koren, "The War on Ukraine Is Testing the Myth of Elon Musk," *The Atlantic*, February 28, 2022, https://www.theatlantic.com/science/archive/2022/02/elon-musk-ukraine-starlink-satellites/622954/ (accessed March 15, 2022).
50. Brandi Vincent, "AI Could Match 'Fingerprints' of Texts to Their Authors, Under New Intelligence Program," Nextgov, February 11, 2022, https://www.nextgov.com/emerging-tech/2022/02/ai-could-match-fingerprints-texts-their-authors-under-new-intelligence-program/361850/ (accessed March 23, 2022), and Mila Jasper, "DARPA Calling for AI Proposals to Measure How Authoritarian Regimes Control Information," June 2, 2021, https://www.nextgov.com/emerging-tech/2021/06/darpa-calling-ai-proposals-measure-how-authoritarian-regimes-control-information/174442/ (accessed March 23, 2022).
51. Bill Gertz, "William Burns Backs CIA AI to Counter China," *The Washington Times*, February 24, 2021, https://www.washingtontimes.com/news/2021/feb/24/william-burns-backs-cia-ai-to-counter-china/ (accessed March 23, 2022).
52. Joshua Baron, "Fight Digital Authoritarianism By Giving People the Tools to Counter It," DefenseOne, June 8, 2021, https://www.defenseone.com/ideas/2021/06/fight-digital-authoritarianism-giving-people-tools-counter-it/174579/ (accessed March 16, 2022).
53. Office of the Director of National Intelligence, "FY2022–2026 ODNI S&T Investment Landscape," Science and Technology Group (STG), Policy and Capabilities Directorate, February 28, 2022, https://sam.gov/opp/15d5927d5c5345939830e882856d2fca/view (accessed March 23, 2022).
54. Thomas Newdick, "This Is the Armada of Spy Planes Tracking Russia's Forces Surrounding Ukraine," The Drive, February 18, 2022, https://www.thedrive.com/the-war-zone/44337/these-are-the-planes-keeping-watch-on-russian-forces-around-ukraine (accessed March 15, 2022).
55. Ibid., and Sanger et al., "Arming Ukraine: 17,000 Anti-Tank Weapons."
56. Ken Dilanian, "Biden Administration Walks Fine Line on Intelligence-Sharing with Ukraine," NBC News, March 4, 2022, https://www.nbcnews.com/news/investigations/biden-administration-walks-fine-line-intelligence-sharing-ukraine-rcna18542 (accessed March 15, 2022).
57. Warren P. Strobel and Michael R. Gordon, "Biden Administration Altered Rules for Sharing Intelligence With Ukraine," *The Wall Street Journal*, March 8, 2022, https://www.wsj.com/articles/biden-administration-altered-rules-for-sharing-intelligence-with-ukraine-11646744400 (accessed March 15, 2022).
58. Ibid.
59. Zach Dorfman, "As the Russian Threat Grew, U.S. Intelligence Ties to Ukraine Deepened," February 2, 2022, https://news.yahoo.com/as-the-russian-threat-grew-us-intelligence-ties-to-ukraine-deepened-225919359.html (accessed March 15, 2022).
60. Ibid.
61. Emily Harding, "Move Over JARVIS, Meet OSCAR—Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community," Center for Strategic and International Studies, January 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220118_Harding_MoveOverJARVIS_MeetOSCAR.pdf?OhpTTFfElnMGwk3Y78lUTyS.2ZueJWMJ (accessed March 15, 2022).
62. Christian Davenport, "Commercial Satellites Push the Rules of War in Russia's Invasion of Ukraine," *The Washington Post*, March 10, 2022, https://www.washingtonpost.com/technology/2022/03/10/commercial-satellites-ukraine-russia-intelligence/ (accessed March 16, 2022).
63. Steve Stransky, "The 2022 Cyber Incident Reporting Law: Key Issues to Watch," Lawfare Blog, March 25, 2022, https://www.lawfareblog.com/2022-cyber-incident-reporting-law-key-issues-watch (accessed April 7, 2022).

64. Christopher Wray, Hearing on Annual Worldwide Threats, U.S. House Permanent Select Committee on Intelligence, March 8, 2022, p. 70, https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Transcript-20220308.pdf (accessed March 31, 2022).
65. Eric Geller, "'TSA Has Screwed This Up': Pipeline Cyber Rules Hitting Major Hurdles," *Politico*, March 17, 2022, https://subscriber.politicopro.com/article/2022/03/tsa-has-screwed-this-up-pipeline-cyber-rules-hitting-major-hurdles-00017893 (accessed March 17, 2022).
66. Cybersecurity and Infrastructure Security Agency, "CISA Hosts Eighth Cyber Storm Exercise with More Than 200 Organizations," March 14, 2022, https://www.cisa.gov/news/2022/03/14/cisa-hosts-eighth-cyber-storm-exercise-more-200-organizations (accessed March 16, 2022).
67. "Black start is the process of restoring power to an electric substation or part of the grid that has experienced a total or partial shutdown without relying on an external power transmission network to get things back online." Defense Advanced Research Projects Agency, "Technologies to Rapidly Restore the Electrical Grid After Cyberattack Come Online," February 23, 2021, https://www.darpa.mil/news-events/2021-02-23 (accessed March 16, 2022).
68. David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *The New York Times*, February 28, 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html (accessed March 17, 2022).
69. Dion Nissenbaum, "Iran Claims Missile Attack on Iraq That Sent U.S. Troops Rushing for Shelter," *The Wall Street Journal*, March 13, 2022, https://www.wsj.com/articles/irans-revolutionary-guard-claims-missile-attack-raising-tensions-11647173230 (accessed April 11, 2022); Timothy W. Martin and Chieko Tsuneoka, "North Korea Test-Fires Intercontinental Ballistic Missile," *The Wall Street Journal*, March 24, 2022, https://www.wsj.com/articles/north-korea-shoots-off-another-unknown-projectile-11648102443 (accessed April 11, 2022); and Lingling Wei and James T. Areddy, "Is China Helping Russia? Beijing-Moscow Relations Explained," *The Wall Street Journal*, April 5, 2022, https://www.wsj.com/articles/russia-china-relations-what-to-know-11647400417 (accessed April 11, 2022).
70. Mari Dugas, "Cyberspace Multiplier: Enhancing Domestic Cyberspace Resiliency with the National Guard," *New York University Journal of Legislation & Public Policy*, February 11, 2022, https://nyujlpp.org/quorum/dugas-cyberspace-multiplier/ (accessed March 15, 2022).
71. Monica M. Ruiz and David Forscey, "The Hybrid Benefits of the National Guard," Lawfare Blog, July 23, 2019, https://www.lawfareblog.com/hybrid-benefits-national-guard (accessed March 17, 2022).
72. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93–288.
73. See Dugas, "Cyberspace Multiplier."
74. Aaron Clarke, "How Often Does the National Guard Respond to Cyberattacks?" Third Way, June 21, 2021, https://www.thirdway.org/graphic/how-often-does-the-national-guard-respond-to-cyberattacks (accessed March 17, 2022).
75. Lora Ries, "DeSantis Aims for Self-Reliance for Florida in Emergencies Instead of Dependence on Feds," Daily Signal, December 7, 2021, https://www.dailysignal.com/2021/12/07/desantis-aims-for-self-reliance-for-florida-in-emergencies-instead-of-dependence-on-feds (accessed March 17, 2022).
76. Colin Wood, "Interstate Cybersecurity Operations Center Is on the Way," StateScoop, January 20, 2022, https://statescoop.com/interstate-cybersecurity-operations-center-north-dakota/ (accessed March 16, 2022).
77. Office of Governor Ron DeSantis, "Governor Ron DeSantis Announces $20 Million to Create Cybersecurity and Information Technology Workforce Education Opportunities," March 2, 2022, https://www.flgov.com/2022/03/02/governor-ron-desantis-announces-20-million-to-create-cybersecurity-and-information-technology-workforce-education-opportunities/ (accessed March 16, 2022).
78. James DiPane, "Cybersecurity: Policymakers Need a Consistent Means to Assess Capabilities," Heritage Foundation *Issue Brief*, August 25, 2021, https://www.heritage.org/defense/report/cybersecurity-policymakers-need-consistent-means-assess-capabilities.
79. U.S. Cyberspace Solarium Commission, *Hardware and Software That Detects or Causes a Change Through the Direct Monitoring and/or Control of Physical Devices, Processes, and Events in the Enterprise*, March 2020, https://www.solarium.gov/report (accessed March 31, 2022).
80. Lisa Ferdinando, "DOD Officials: Chinese Actions Threaten U.S. Technological, Industrial Base," *DOD News*, June 21, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1557188/dod-officials-chinese-actions-threaten-us-technological-industrial-base/ (accessed March 31, 2022).
81. Luis Martinez et al., "Major U.S. Weapons Compromised By Chinese Hackers, Report Warns," ABC News, May 28, 2013, https://abcnews.go.com/Blotter/major-us-weapons-compromised-chinese-hackers-report-warns/story?id=19271995 (accessed March 31, 2022).
82. John Slye, "Defense Cybersecurity Provisions in the Final 2022 National Defense Authorization Act," December 16, 2021, https://iq.govwin.com/neo/marketAnalysis/view/Defense-Cybersecurity-Provisions-in-the-Final-2022-National-Defense-Authorization-Act/6310?researchTypeId=1&researchMarket= (accessed March 31, 2022).
83. Todd Harrison, "Commercial Space Remote Sensing and Its Role in National Security," Center for Strategic and International Studies, February 2, 2022, https://www.csis.org/analysis/commercial-space-remote-sensing-and-its-role-national-security (accessed March 17, 2022).