



(PST Vector / Shutterstock)

What America Learned from Cyber War in Ukraine—Before the First Shots were Fired

How pre-existing U.S. investments, partnerships, and planning bolstered Ukraine's efforts to defend itself online—and how much more might have been done.

By Mary Brooks, Wilson Public Policy Scholar



**Science and Technology
Innovation Program**

This analysis was written in the author's role as a public policy scholar at the Wilson Center. The views and opinions presented herein are those of the author and do not necessarily represent the views of the State Department.

Contents

- Author Notes** **3**
- Setting the Stage: Ukraine in 2014** **4**
- The Early Years (2013-2016):
Congress, the U.S. Government, and NATO** **5**
- The Early Years (2013-2016):
Private Sector** **7**
- A (Partial) Wake-Up Call** **8**
- 2017–Early 2021: Collaboration Efforts Gather Steam** **9**
- Fall 2021–February 2022:
Preparing for War** **11**
- Lessons Learned** **13**
 - 1. Some Political and Legal Changes Are Impossible Until War Actually Begins. . . . 13
 - 2. Commercial Companies Make the Difference—
and Occasionally Introduce New Challenges. . . . 14
 - 3. Talented, Dedicated Volunteers Can Have an Outsized Impact 15
 - 4. Pre-Existing Partnerships Make An Enormous Difference 16
 - 5. International Cyber Assistance Efforts Remain Early-Stage 16
 - 6. Cybersecurity Has No Silver Bullet 17
- Conclusion** **18**
- Endnotes** **19**

When the first Russian tanks crossed into Ukraine in February 2022, the United States and its allies rushed in aid, weapons, and intelligence to help Kyiv defend itself. Yet even as they were coming in, another group was just leaving: a team of several dozen American analysts and operators sent by U.S. CyberCommand in an eleventh-hour effort to secure Ukraine from the anticipated digital onslaught.¹ For more than two months, the CyberCommand team members worked side by side with their Ukrainian counterparts to identify vulnerabilities across three of the country's major networks and to suggest possible remediations.

They weren't alone. In the weeks, months, and even years preceding the invasion, a loosely-coordinated array of American cybersecurity companies, military actors, government agencies, and private individuals stepped in to help Ukraine, long before it was obvious that full-scale war would break out. American partners funded new training environments, worked with the Ukrainian military to centralize controls across its segmented networks, and identified vulnerabilities. They offered technical support and training, shaped government cybersecurity strategies, and tried to kickstart a dynamic private cybersecurity environment in Ukraine—one modeled after Israel's famously vibrant and strong industry.

These diverse actors pioneered the bulk of early American efforts to provide cybersecurity assistance to a major non-NATO ally. Unsurprisingly, their learning curve was at times steep. While the muscle memory for delivering food aid or weapons to another country is long-established, cybersecurity aid is a new and deeply technical form of support. It is often treated as a national security issue and thus shrouded in secrecy, and it is heavily reliant on the commercial private sector, as opposed to an established defense industrial base. And so, as Americans and other allies strove to help Ukraine, they ran into new challenges and discovered the limits of their ability to influence the direction of the cybersecurity environment of a different country.

And so as Americans and other allies strove to help Ukraine, they ran into new challenges and discovered the limits of their ability to influence the direction of the cybersecurity environment of a different country.

When full-scale conflict broke out in February 2022, this pre-war effort, with all its strengths and weaknesses, was put to the test by Russian and Russian-affiliated hackers. Wipers—designed to “wipe” data permanently—targeted Ukrainian government and civilian networks. Disinformation operations were launched at domestic and foreign populations alike. Critical infrastructure was attacked: most notably the 2022 takedown of the American satellite internet company Viasat—which operated in Ukraine and Europe—and the major telecommunications giant Kyivstar in late 2023.² Groups of volunteer “patriotic hackers” parried back and forth in digital space. By late 2022 and into 2023, there were reports that NATO territory was facing limited, though destructive, attacks against transportation and logistics infrastructure.

But the most remarkable element of the digital war to date is what has not been seen: cyberattacks do not appear to have substantially turned the tide of the conflict.³ Much of Ukraine's critical communications, transportation, and Internet infrastructure has remained online—and when taken offline, has been the consequence of physical (kinetic) attacks. Military command and control has been retained. Ukrainian president Volodymyr Zelensky, famously, can communicate with the majority of his population as well as the world beyond.⁴

How much of this dynamic can be directly attributed to America's pre-war international cybersecurity assistance efforts is unclear. Russian hubris and under-preparation, Ukrainian talent, and the realities of prosecuting a war all play a role. Yet the digital war in Ukraine has become in some ways a proving ground for early American international cybersecurity assistance efforts. It offers an occasion to evaluate which partnerships and investments paid off when conflict broke out, which appear to have had little impact,⁵ and where opportunities were missed.

But the most remarkable element of the digital war to date is what has not been seen: cyberattacks do not appear to have substantially turned the tide of the conflict.

In a world in which the importance of digital connectivity on the battlefield and beyond will only grow, America's pre-war efforts to provide cybersecurity assistance to Ukraine present important lessons. They offer a template, albeit an imperfect one, for how America thinks about its national interests and its capabilities. And they provide both a warning and an opportunity, at a moment Beijing is making its own evaluation: examining Taiwan's digital defenses as well as America's ability to come to the support of a country under threat half a world away.

What follows is a two-part examination of the lessons that America should draw from the experience of helping Ukraine's cyber defenders prepare for war. The first is an overview of what American cybersecurity assistance to Ukraine looked like between 2012 and the outbreak of war in 2022. The second part analyzes these efforts in the context of the war and offers some high-level conclusions to drive the present and future of American cybersecurity aid.

Address by President Volodymyr Zelenskyy. (President Of Ukraine / Public Domain)

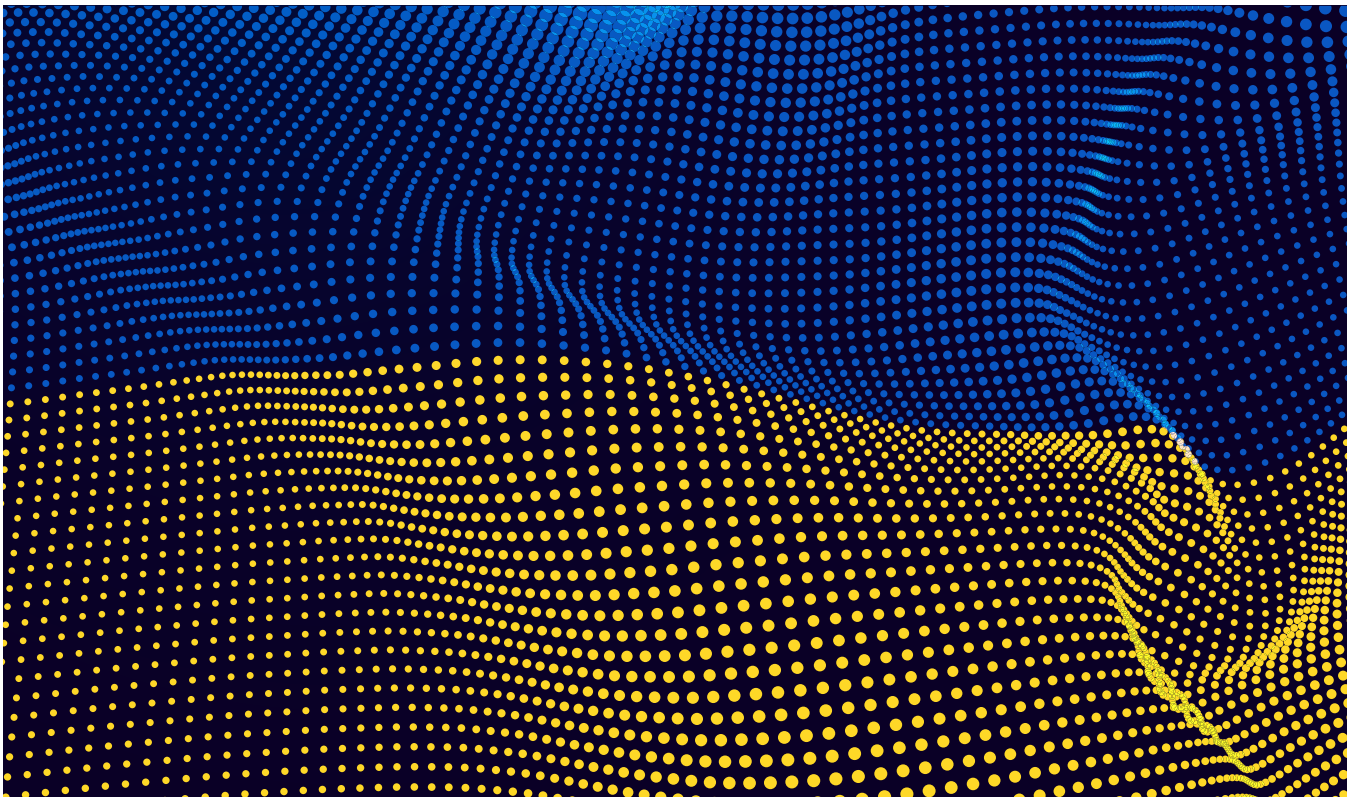


Author Notes

Methodology—This analysis relies on existing public information and on interviews with key American cybersecurity stakeholders including current Biden Administration officials, current and former cybersecurity company employees, current and former military officials and civilian contractors, analysts, and entrepreneurs. Some of these were exclusive to this research project, and some were in the course of reporting for a forthcoming book, *New Cold Wars*.⁶ Several interviewees gave permission for their names to be used, and these are noted in the text. Most, however, spoke on the condition of anonymity. When anonymous sources are cited in the footnotes, every effort is made to complement the private-source information with public reporting.

Scope—The cyber war in Ukraine is being fought in many arenas: in space, on the ground, at home, and internationally. This particular analysis focuses solely on the United States’ perspective, as communicated by the interviewees, on cyber war in Ukraine. This does not in any way discount the initiative, innovation, and achievements of Ukraine’s cyber defenders. For years, Ukrainians worked to build up their country’s digital defenses: investing in new infrastructure, seeking out partnerships at home and abroad, and taking advantage of their own talented domestic cyber force to build a strong IT industry. Everyone interviewed for this analysis agreed that Ukrainians undertook the vast majority of the work conducted on their own systems with unique creativity. What is especially notable about several of these initiatives is how much progress Ukrainians were able to make while operating at vastly lower budgets and with much less infrastructure than United States equivalents and how creatively private-sector entities and public sector agencies collaborated with each other.

Ukraine flag. (SkillUp / Shutterstock)



Setting the Stage: Ukraine in 2014

On March 18, 2014, Russia annexed the Crimean Peninsula. By this time, cyber war in Ukraine was already well underway.

Prior to 2012, cyberattacks against the country's infrastructure constituted—in the words of Nikolay Koval, the former head of Ukraine's emergency-response team⁷—"a fairly typical array of incidents."⁸ Yet starting in 2013, he noted, exploitation operations were becoming more severe. American threat intelligence companies began tracking and observing state-sponsored espionage campaigns that could be traced to Russia's internal security service, the FSB.⁹ It didn't escape anyone's notice that many of these operations seemed timed to delicate political moments in Ukraine, such as ongoing 2013 deliberations about whether Ukraine would align itself more closely with the European Union.

By late spring 2014, outright cyberattacks were escalating—right as popular protests against then-President Viktor Yanukovich, widely seen as corrupt and unduly influenced by Russian president Vladimir Putin, grew. Ukraine was hammered by relatively unsophisticated but plentiful attacks, including a major distributed denial of service campaign (DDOS) that took down government websites. Most famously, pro-Russian hackers went after the May 25, 2014 Ukrainian presidential election, installing a virus onto the computers of the Central Elections Commission that would have reported the vote tally incorrectly when the results were publicized.¹⁰ While this would not have changed the results of the election, it would have shown the extreme far-right candidate as the winner—likely casting doubt on the integrity of the electoral process. Ukrainian defenders caught the malware only minutes before the falsified results would have gone public. (Shortly afterward, Russian state-run TV aired the "results" of the Ukrainian election, giving the exact percentage that would have been reported by the malware.¹¹)

Over time, the shock of the Crimean invasion faded from American minds. But the shooting war in eastern Ukraine—and the digital effects that accompanied it—became endemic. Thousands of cyberattacks blasted Ukrainian networks each month.¹² In the east, information warfare became a part of everyday life: surprising soldiers in the trenches who received text messages telling them to retreat—and sometimes claiming their fellow soldiers had already done so.¹³

Contemporaneous accounts of Ukraine's cybersecurity defenses during this era¹⁴—published in a NATO-sponsored book entitled *Cyber War in Perspective*—paint a picture of a country that was generally unprepared at all levels to meet the challenges posed by sustained state-backed malicious cyber operations.¹⁵

While Ukraine was already well-known for the creativity and skill of individual cybersecurity experts and IT sector, the government workforce struggled: reliant on under-skilled, under-resourced, and underpaid employees.¹⁶ Ukraine had no updated cybersecurity strategy: key policy and legal documents dated back to the Soviet days, and the regulatory environment around cybersecurity was virtually non-existent.¹⁷ Meanwhile, various government

In the east, electronic warfare became a part of everyday life: even soldiers in the trenches received text messages telling them to retreat—and sometimes claiming their fellow soldiers had already done so.

agencies and cells tasked with cybersecurity functions operated autonomously and without a central coordinating structure. Information wasn't shared, and infighting was endemic—sometimes disagreements broke out in front of foreign allies.¹⁸

When it came to infrastructure, the conclusions were particularly challenging: The Ukrainian government relied heavily on Russian companies, products, and expertise—including for web resources like social media and email, software, and hardware.¹⁹ Basic technical solutions, such as tools that would have blocked DDOS attacks from Ukrainian internet infrastructure or ensured that Ukraine's digital space could be monitored, were not in place.²⁰ The country suffered from a lack of broader “cyber hygiene”—general adherence to standard security practices.

Ukraine's lack of a sophisticated national cybersecurity defense capability was not uncommon for the era. In the mid-2010s, the whole world was still learning the importance of cyber power, in all its incarnations, and how it could be used to disrupt societies and undercut military operations.²¹ What it did mean, however, was that Ukraine—which was quickly becoming the favorite target of Putin's hackers—had a long way to go.

The Early Years (2013-2016): Congress, the U.S. Government, and NATO

During the majority of former President Barack Obama's second term, U.S. stakeholders were often far less concerned about Russian cyberattacks than they were Ukrainian ones. At the time, Ukraine was one of the worst hotbeds of cybercrime in the world. Most memorably, the malware used in one of the most well-known early U.S. security incidents—the 2013 Target breach that affected over 100 million customers—was traced in part back to a Ukrainian actor.²²

Army troops transporter and tank with Ukrainian flag, Ukraine. (Milan Sommer / Shutterstock)



So when Congress convened in the wake of the Crimea annexation in 2014 to discuss aid to Ukraine, they focused less on helping Kyiv with its own networks and instead on stamping out cybercrimes that emanated routinely from the country. Notably, in March 2014, Senators Mark Warner (D-VA) and Mark Kirk (R-IL) co-sponsored an amendment to launch a major collaboration between the United States and Ukraine to tackle cybercrime.²³ Ultimately, this amendment wasn't included in the general aid bill,²⁴ but a watered-down version was included in a later intelligence authorization bill. This established that it was the "sense of Congress" to improve coordination between the two countries on cybercrime. The law identified a series of early steps to take, including efforts to "increase" intelligence and law enforcement cooperation with Ukraine, "improve" extradition procedures of cybercriminals, and extract a commitment from the government of Ukraine to end international cybercrime.²⁵ This appears to have been the first major non-military initiatives between the two countries in cybersecurity.

Apart from Congress, the major government cybersecurity collaboration in the early part of this era came mainly from the U.S. and Allied militaries. Since the late 1990s, NATO-Ukraine cooperation and collaboration had been channeled through a NATO-Ukraine Commission.²⁶ But after 2014, the work kicked into higher gear: at that year's summit, NATO allies agreed to deepen their support for Ukraine in a variety of areas, including through a "trust fund" dedicated specifically to cyber defense.²⁷ Notably, the effort was short-term—issued originally for a 30-month contracting period—and had a "strictly defensive" mission.²⁸ Led by Romania, the fund focused on advising Ukraine and providing equipment for training. On the Ukrainian side, the fund was coordinated by the security service of Ukraine, the SBU.

In 2016, this fund was folded into a Comprehensive Assistance Plan for Ukraine, which additionally included a mandate to help Ukraine modernize its C4 capabilities (Command, Control, Communications and Computers)²⁹ and to ensure material interoperability and information-sharing between Ukraine and NATO. It also aimed to help Ukraine develop laboratories to investigate major incidents and to help secure critical infrastructure.

U.S. Secretary of State John Kerry listens as NATO Secretary-General Anders Fogh Rasmussen opens a special discussion about Ukraine at NATO Headquarters in Brussels, Belgium, on June 25, 2014. (U.S. Department of State /Public Domain)



It is difficult to analyze the ultimate impact of this NATO programming, given the sensitivities around military, cyber, and the ongoing conflict. But it is clear that as NATO countries learned how to provide cybersecurity defense support to a non-NATO ally, they ran into challenges—often of their own making. When, for example, Romania tried to export equipment to Ukraine, they were slowed down by their own export control regime, which classified some of the materials as dual use and required a permit, and by EU sanctions, which forbid the export of goods into Crimea or Sevastopol.³⁰

According to General Tod Wolters, who was serving at the time as the Supreme Allied Commander Europe from 2019 to 2022, NATO’s role in providing cybersecurity training and support to Ukraine was “not as robust” as that of the U.S. and individual countries in Europe.³¹ Where NATO investments had an impact, he suggested, was in creating channels for allied and Ukrainian partners to collaborate. “Efforts by several NATO nations—to include the U.S., U.K., and Estonia—to construct channels of communication, and to tend to the cyber hygiene of military networks were ‘force multipliers’ for European security,” Wolters recalled. “What this did was teach western military and Ukrainian forces how to work with each other and to maintain communication.”³²

The Early Years (2013-2016): Private Sector

During these years, private U.S. companies worked in Ukraine—often in the context of regular business operations. Google established a Kyiv office in 2006.³³ Microsoft established one in 2003.³⁴ While it was mostly established for direct customer support and marketing purposes, the ubiquitous nature of Microsoft’s software for government and private use meant that the company had visibility into goings-on in Ukraine and could notify victims of hacking. iSight Partners, a cyber threat intelligence firm acquired by Mandiant, made U.S. news on several occasions with its investigations identifying threat actors’ exploitation of vulnerabilities in Ukraine.³⁵

The main goal of these partnerships was commercial gain, and not to bolster Ukraine’s cybersecurity in a geopolitical sense or with an eye toward potential nation-state conflict. Yet these investments had an outsize impact because—unlike the United States, which has its long-established bespoke defense industrial base—Ukraine more frequently turns to commercial solutions for government and national security procurement. Thus, these companies also served to build key relationships with the government and commercial sectors in Ukraine that could—and would—be drawn on when the war broke out.

Thus, these companies also served to build key relationships with the government and commercial sectors in Ukraine that could—and would—be drawn on when the war broke out.

There was something in it for the companies as well. One former employee of a networking company who visited Ukraine multiple times for his company, characterized the situation thus: “What we saw there [in terms of malware] was 3-4 years ahead of what would be used elsewhere. Russia used Ukraine for a testing ground, so we would get to see [new Russian tactics] in advance... it was a win-win.”³⁶

In general, individual Americans who worked on Ukrainian cybersecurity issues during these years all agreed on two things: 1) that Ukraine’s overall cybersecurity environment at the time was terrible and 2) that Ukrainian cyber experts, individually, were some of the most talented they’d ever worked with.

A (Partial) Wake-Up Call

In 2015, the United States got a wake-up call. Halfway around the world, in central Ukraine, hackers had shut off part of the power grid near Kyiv in the middle of the winter, just two days before Christmas, in an incident that would later be attributed to the Russian SVR. Some 200,000 customers, from three energy companies, were left in the cold.

Overall, the incident was not particularly memorable for average Ukrainians. Customers only lost power for a few hours, and the grid takedown was one of tens of thousands of cyberattacks that emanated from Russia in the wake of the Crimea annexation and ongoing war in the East. But for the cybersecurity community in the United States and in Ukraine, it was seen as a watershed moment.

This was one of the rare times that a cyberattack was used to target the industrial control systems that constituted civilian critical infrastructure.³⁷ More significantly, this was the first public report of a cyberattack taking down a power grid, and in the United States, people were eager to learn what had happened and why. Several teams from the United States, including government interagency teams and non-government information-sharing associations, deployed to Ukraine to interview employees of the impacted companies, meet, and work with government counterparts, and learn more about the incident.³⁸

This was one of the rare times that a cyberattack was used to target the industrial control systems that constituted civilian critical infrastructure.

In 2016, it happened again: A week before Christmas, Russian hackers again shut down part of the Ukrainian power grid—this time, going after an electrical substation which potentially could impact a far broader range of consumers.³⁹ As with the previous year's attack, the grid was promptly brought back online. Yet this time, it appeared that the malware wasn't just designed to cause a blackout but to permanently damage key parts of the power grid, causing physical and long-lasting damage.⁴⁰

The grid attacks were one of the inflection points in the relationship between Ukraine and the United States—perhaps not so much for Congress but rather for the executive branch. The federal government, recalled Eric Goldstein, who currently serves as the Cyberspace and Infrastructure Security Agency (CISA) Executive Assistant Director for Cybersecurity, established a “whole-of-government collaboration” effort with Ukraine to “help them assess the security of their critical infrastructure.”⁴¹ These efforts aligned with a strong Ukrainian response. “Subsequent to those events in 2015 and 2016,” Goldstein continued, “Ukrainians made extraordinary investments, in part enabled by the international community, and in part because of their own increasing awareness of their vulnerability to improve both the resilience and the detection across their networks.”⁴²

Still, there was one more major catalyst left: the *NotPetya* attacks that swept across Ukraine—and later the world—in the summer of 2017. This remains the costliest cyberattack to date, as Russian hackers weaponized a vulnerability in a widely-used Ukrainian tax accounting software to cripple firms and government agencies across the country—including banks, railways, and multinational companies. Even the monitoring systems at the Chernobyl nuclear plant went offline. Yet while *NotPetya* masqueraded as a ransomware attack, analysts reported that there was no recovery key: this was designed to maximize destruction and not for financial gain.⁴³

The scope astonished American officials, who realized that an attack this damaging could easily happen again—and that what happened in one country would not remain there.

2017–Early 2021: Collaboration Efforts Gather Steam

Starting around 2016–2017, cybersecurity support to Ukraine from the U.S. private and public sector picked up speed. It is unclear whether it was catalyzed by the power grid incidents or *NotPetya*, a function of Ukraine’s own initiative on improving its cybersecurity, or simply reflected America’s own evolution.

Between 2017 and early 2021, U.S. government support can generally be grouped by function:

First was the ongoing **institution-to-institution collaboration and capacity-building**. This can be categorized as operational support by peer organizations and counterparts, as opposed to strategic or policy focused efforts. Some of the gold-star work in this space, according to several interviewees, was conducted in the energy sector by entities like the Department of Energy and the Idaho National Laboratory, who collaborated with counterparts in Ukraine on incident response and hardening of defenses.⁴⁴

Other collaborations existed: The U.S. Treasury worked with the National Bank of Ukraine “to improve cybersecurity information sharing and on discrete projects.”⁴⁵ Two trade and advocacy organizations—the United States Energy Association and the National Association of Regulatory Utility Commissioners—established a regional program in Eastern Europe designed to bolster the security of the power grid.⁴⁶ The Department of Homeland Security provided operational assistance, both through CISA and through its predecessor agency. Working with the computer emergency response team of Ukraine, CISA described its work as aimed at helping them to develop collaboration mechanisms, governance platforms, and information-sharing processes.⁴⁷

Another category was a combination of **diplomatic and strategic efforts**, headed by the Department of State. Some of this work supported Ukraine’s efforts to rewrite its first national cybersecurity strategy, a task which was conducted by Ukraine’s National Security and Defense Council and issued by decree by President Zelensky in May 2021.⁴⁸

Other work centered around a series of annual “U.S.-Ukraine Cyber Bilateral Dialogues.” These conferences, held in September 2017, November 2018, and March 2020 served as a forum to unite key government leaders from both countries and as an opportunity for the United States to publicly commit to new funding—at least \$18 million dollars over the course of the three events.⁴⁹ Joseph Pennington, who served as the top U.S. diplomat in Ukraine at the time, noted that Ukraine was one of the few countries with which the U.S. held this type of cyber engagement. It was important, he said, for two reasons: one, to stand with Ukraine to resist Russian aggression; and two, because

This remains the most costly cyberattack to date, as Russian hackers weaponized a vulnerability in a widely-used Ukrainian tax accounting software to cripple firms and government agencies across the country—including banks, railways, and multinational companies.

what happened in Ukraine would spread to the rest of the world—as it had in *NotPetya*. It was clear that improving cooperation and information-sharing in advance of an emergency was in everyone’s best interests.⁵⁰

Another major initiative was a 2019 program launched by non-profit consultancy CRDF Global, which broadly aimed to strengthen the cybersecurity environment in Ukraine by working directly with representatives of Ukraine’s National Security and Defence Council.⁵¹ This partnership led to the 2021 creation of a “National Cybersecurity Cluster,” which bills itself as a “strategic coordination platform” that brings together various national and regional cybersecurity actors in Ukraine on a routine basis to share information and synchronize programming.⁵²

Some efforts to increase diplomatic cybersecurity aid to Ukraine in this era failed. For example, Senator James Risch (ID) introduced at least two bills in 2021 that would have earmarked \$50 million dollars a year, from 2022 - 2026, to fund a State-Department-lead initiative on cybersecurity, anti-corruption, and other security initiatives in Ukraine.⁵³ These did not pass. However, the original Congressional imperative—the need to fight cybercrime emanating from Ukraine—is at least somewhat on track: In 2020, the FBI praised Ukraine’s “unrelenting efforts ... to arrest and extradite cybercriminals who operated freely in Ukraine for many years.”⁵⁴

The third type of international cybersecurity assistance effort was centered around the **military and defense of military networks**. In addition to work funneled through NATO, U.S. soldiers were also working directly with counterparts through U.S. European Command (EUCOM) to help Ukrainian forces to build up their cyber defenses. Their job was to work closely with the State Department, through the defense attaché, to support Ukraine in a wide array of engagements, ranging from humanitarian support, to joint training, to efforts to harden military cybersecurity.⁵⁵ Some of this work was completed through security assistance programs, such as the U.S. Army’s Security Assistance Training Management Organization.⁵⁶ In June 2020, the Defense Department announced \$250 million in funding, some of it dedicated to cyber defenses, would be funneled through its ongoing Ukraine Security Assistance Initiative.⁵⁷

The National Guard efforts were described by both military and intelligence interviewees as some of the most long-term consistent and fruitful engagement with Ukraine in this space.

Notably, several of the boots-on-the-ground cyber operators based in Ukraine came from a seemingly unlikely origin: the California National Guard, which has a three-decade-old partnership through the National Guard’s State Partnership Program.⁵⁸ Soldiers affiliated with the California National Guard rotated into Ukraine to offer digital support and training to local forces and to help them build out their cyber networks. For example, around 2020, CA National Guard soldiers were on the ground in Europe, supporting Ukraine’s efforts to increase insight into their military networks, and to combine controls across a number of smaller networks to facilitate information-sharing and

interoperability.⁵⁹ The National Guard efforts were described by both military and intelligence interviewees as some of the most long-term consistent and fruitful engagement with Ukraine in this space.⁶⁰

It was clear that improving cooperation and information-sharing in advance of an emergency was in everyone’s best interests.

Beginning in 2018, CyberCommand began to send its “Hunt Forward” mission teams around the world—and to Ukraine. Their job was to secure local authorities’ permission to place sensors on the networks of key critical infrastructure and/or government entities—in an effort to discover vulnerabilities that Russian cyber operatives might well try to exploit—and then to offer some recommendations for how Ukrainians might patch them.⁶¹ However, these mission teams do not themselves conduct any remediation efforts.

The fourth line of effort was certainly the most publicized: a \$37 million dollar, first-of-its-kind broad cyber support project run by USAID to **strengthen the country’s civilian cybersecurity ecosystem**. In 2016, USAID had launched a smaller program whose goal, in part, was to strengthen the cybersecurity of elections infrastructure in Ukraine.⁶² But what began in 2020 was an order of magnitude more ambitious: the Cybersecurity for Critical Infrastructure program, focused on “strengthening the cyber environment, developing a cybersecurity workforce, and building a resilient cybersecurity industry.”⁶³ USAID had never run a cybersecurity program before. The original agency announcement⁶⁴ did not specify a certain amount of funding or specific goal: instead, the project was initiated through a “co-creation” process in which experts, investors, or organizations could apply to participate in developing the proposal together, in the summer of 2019.⁶⁵

The program’s goals, according to those familiar with its design, were lofty. Essentially, one of the questions asked was whether Ukraine could be made more like Israel—a country with a famously powerful cybersecurity ecosystem. Ultimately, the program achieved certain goals—like embedding technical experts in the government of Ukraine, and “deploy[ing] cybersecurity software and hardware tools to ensure the resilience of critical infrastructure to physical and cyber attacks”—and established a new series of cybersecurity dialogues.⁶⁶ However, the COVID pandemic caused the suspension of a number of operations, and these were not fully back in place even before the war broke out, so it is difficult to evaluate the positive impact of this grant fund. Privately, several American and Ukrainian stakeholders interviewed for this analysis said that it was difficult to fit all the qualifications in order to receive aid, and that they weren’t actually sure where the money was spent.⁶⁷ It is also clear that this was a long-term capacity building project for the nation’s cybersecurity industry, and not designed to remediate the most immediate cyber challenges facing Ukraine.

Fall 2021–February 2022: Preparing for War

In late fall of 2021, as it became increasingly clear to the United States intelligence community that Russia was preparing to invade Ukraine, the tenor of cybersecurity support efforts changed. The imminent prospect of war began to make solutions that were previously politically or logistically untenable a viable possibility, as national security experts braced themselves for war.

Deputy National Security Advisor Anne Neuberger flew across the Atlantic to warn NATO allies to secure their own networks.⁶⁸ American officials feared if war broke out, Russian President Vladimir Putin might branch out and use cyberattacks against European countries to undercut their ability to support Ukraine—leading to another *NotPetya* scenario.⁶⁹ At CISA, officials were busy thinking about the ways that the United States might protect itself digitally—and where its weaknesses were. This work would manifest itself in late February 2022 in CISA’s “Shields Up” campaign, warning U.S. companies to be on the lookout for a spike in malicious Russian activity.

Meanwhile, at Cyber Command and the National Security Agency, General Paul Nakasone dispatched another Hunt Forward team to western Ukraine. This was the fourth trip to Ukraine, but the first time that a team had deployed in the immediate run-up to ground combat. As such, it carried a sense of urgency that previous missions to the country had not.⁷⁰ Operators remained on the ground for approximately 70 days: living in hotels and working alongside Ukrainian cyber operators in critical infrastructure and government to identify vulnerabilities that the Ukrainians then remediated.⁷¹ The team was present while a January 2022 wave of disruptive cyberattacks targeted government systems, and returned to the United States several weeks before the invasion.

Finally, America’s largest cyber and technology companies were also bracing for a digital conflict.⁷² As the geopolitical tensions ratcheted ever-higher, Microsoft stood up a cross-company task force of about 100 people to focus on the coming potential conflict in Ukraine, to sort out how to quickly communicate across teams, and to prepare for any fallout.⁷³ In mid-January, they got the first taste of what that conflict might look like from the wave of disruptive attacks aimed at Ukrainian government networks: a campaign they called “WhisperGate.”⁷⁴ They quickly warned the White House, who put them in touch with Ukrainian counterparts. A month later, on February 23rd, another digital attack spread across government infrastructure in Ukraine—this one bigger in scope. The war was about to begin.

Aerial photograph of the National Security Agency in Fort Meade, Maryland, 2013 (Trevor Paglen, distributed under a CC0 1.0 license)



Lessons Learned

Efforts to make Ukraine more secure in cyberspace began long before there was the expectation of a full-scale Russian invasion. Yet the ongoing conflict offers an opportunity to draw some conclusions about what early-stage preparations made the most impact once the shooting war began, and to let that analysis shape future efforts to deploy cybersecurity assistance to potentially vulnerable countries. Below are several high-level lessons that have become evident over the past two years of open conflict.

1. Some Political and Legal Changes Are Impossible Until War Actually Begins

When war broke out in Ukraine, several long-standing areas of disagreement were resolved with breakneck speed. “There are things that become only possible in a war context,” said one current government official who was interviewed for this paper.

Many of the most significant of these changes were legal or procedural. One was the ramp-up of information and intelligence from the United States and allied countries to Ukraine. While the details of this intelligence sharing are closely guarded, it is clear that U.S. cyber and military leadership and Ukrainian leadership are collaborating and sharing information—sometimes in almost real time. Private companies are also sharing information about cyberattacks and threats with Ukrainian leadership.⁷⁵

Another example was the rapid transition, supported by American tech companies, of sensitive Ukrainian government data out of the country. Prior to the invasion, security experts had been urging the Ukrainian government to move key data from servers physically located in the country to ones located outside it. This way, Ukraine could still access data using the cloud—even if its physical servers and data centers were destroyed in the fighting—while preventing sensitive information from falling into Russian hands. Yet at the time, this type of data migration was banned by Ukrainian law.⁷⁶ Once the invasion happened, Ukraine’s parliament changed the law, and American tech companies—namely Microsoft and Amazon Web Services—stepped up to help transfer the data.⁷⁷ This was a key decision: within days, one of the major servers on which government data was stored in-country was destroyed by Russian fire.⁷⁸

Once the invasion happened, Ukraine’s parliament changed the law, and American tech companies—namely Microsoft and Amazon Web Services—stepped up to help transfer the data. This was a key decision: within days, one of the major servers on which government data was stored in-country was destroyed by Russian fire.

Other legal changes stemmed from the imposition of martial law in Ukraine, which subordinated the National Guard of Ukraine—which falls with Ukraine’s Ministry of Internal Affairs and exercises a cybersecurity investigative function roughly equivalent to the American FBI—to the Armed Forces. This organizational move changed how the U.S. military could interact with the National Guard, one American military official recalled. When the Guard was considered a “police force,” the U.S. military couldn’t support it. Now, it was a military organization and could be treated as such.⁷⁹

2. Commercial Companies Make the Difference—and Occasionally Introduce New Challenges

The United States' national security apparatus is accustomed to operating with technologies designed by the western defense intelligence base often uniquely for military use. In Ukraine, by contrast, commercial systems are extensively used to prosecute the ongoing conflict. The benefits to Ukraine are clear: it can be much quicker and cheaper to acquire commercial technology, especially in a crisis scenario; the technologies are often cutting-edge; and there are a broad variety of options available. "It is difficult to overestimate the impact that private companies have had in this war," wrote researchers at the European Council on Foreign Relations.⁸⁰

At the same time, there are risks to a heavy dependence on private commercial technology companies—particularly those that are headquartered in foreign countries. In the case of Ukraine, many American technology companies sided clearly with Ukraine, donating millions' worth of free services. Yet variations in their corporate structure, type of service or product, and reasons for support may all affect their staying power as a conflict continues.⁸¹

At the same time, there are risks to a heavy dependence on private commercial technology companies—particularly those that are headquartered in foreign countries.

One of the most illustrative examples of the promise and peril of corporate dependence is the Ukrainian military's reliance on Starlink. Early in the war, when Russian cyberattacks took out the Viasat satellite infrastructure, they also undercut a substantial proportion of the Ukrainian military's ability to communicate. Enter Starlink: the low-earth orbit satellite constellation owned and operated by Elon Musk's SpaceX. Starlink kits, which had not originally been a part of the U.S. or Ukrainian military planning for Ukrainian defenses, were shipped into the country through the border with Poland.⁸² They enabled wide-spread communications between military and civilian leadership. Much of the terminals and ongoing satellite connectivity was donated by Starlink itself.⁸³

Starlink was a game-changer, several government officials interviewed for this analysis said. Ukraine's military and government communications did not run exclusively over Starlink terminals, but they provided the vast majority of connectivity, enabling everything from direct military operations to battlefield communications. Yet there was a catch: Ukraine's ability to use the system relied on Musk's whims. Complaining that he wasn't being paid for ongoing service, he threatened to cut off Ukrainian access.⁸⁴ On at least one occasion, he claimed he personally blocked Starlink connectivity to impede a Ukrainian military operation that he alleged risked escalating the war—a unilateral decision based on a private conversation with the Russian ambassador.⁸⁵ In Washington, interviewees were divided on whether Musk's decision was justified: on one hand, Musk was adjudicating foreign policy decisions himself, almost as a shadow national security official. On the other, it was clear that Musk's own commercial assets were at stake, and that he had the right to make his business decisions accordingly.

When the war began, other elements of the American private sector kicked into gear—mostly with quieter headlines. American tech companies like Google and Microsoft poured resources into figuring out how to rework their service offerings to help the Ukrainian people while undercutting Russian forces. These efforts ranged from financial—offering free software and services to the Ukrainian government and its defenders—to retooling certain

products. For example, in the opening days of the conflict, corporate executives at Google met to discuss how Google Maps could be displayed in a way that would enable Ukrainians to use the technology, without tipping off the Russian invaders about how to attack the fleeing civilians who would be revealed by the red lines that typically denote heavy areas of traffic.

Several companies also created new partnerships to help magnify their impact, and to figure out how to deploy their contributions to be most useful to Kyiv. One of the most

significant in the space is the Cyber Defense Assistance Collaborative (CDAC), which was founded to offer a broad range of top-notch American cybersecurity support directly to companies in Ukraine.⁸⁶ This included, CDAC representatives said, everything from support in designing infrastructure and security operations centers to attack surface monitoring, consulting services, threat analysis, and access to technical resources.⁸⁷

One of the most significant in the space is the Cyber Defense Assistance Collaborative (CDAC), which was founded to offer a broad range of top-notch American cybersecurity support directly to companies in Ukraine.

3. Talented, Dedicated Volunteers Can Have an Outsized Impact

One of the most striking aspects of the digital war in Ukraine is how volunteer-initiated efforts bore fruit years later—and sometimes in unexpected ways.

A prime example is that of Aerorozvidka: a volunteer NGO Ukrainian group of drone operators who banded together in 2014. The team originally collaborated closely with the Ministry of Defence to develop aerial surveillance and intelligence-gathering capabilities and was later formally incorporated into a recognized military unit, A2724.⁸⁸ A2724 pioneered the early integration of aerial reconnaissance efforts into military operations in Ukraine, and initiated the creation of the Ukrainian military situational awareness system, “Delta.” Delta, which received western funding, was designed in collaboration with American forces and aligned to NATO specifications.⁸⁹ In 2022, it was revived and updated for active use on the battlefield, giving Ukrainian forces an advantage in their ability to transmit information in the field more rapidly than Russian counterparts. Innovations like Delta have led several Ukrainian cybersecurity officials to note that Ukraine has become a testing ground for major new weapons platforms, techniques, and intelligence sharing processes, and to point out that Kyiv’s allies—before and during the war—have sought to learn from Ukrainian examples.⁹⁰

Other volunteer organizations sprang up—particularly once conflict broke out—and drew only on the support of hackers around the world but also the wealth of talent inside the country’s borders. One notable organization is the “IT Army of Ukraine”, a hacktivist⁹¹ group of civilian volunteers called up by Ukraine’s Digital Minister, Mykhailo Fedorov with the mandate to conduct offensive digital operations in defense of Ukraine. The “IT Army” has conducted a wide variety of operations, from attacking physical infrastructure in Russian-controlled areas of east Ukraine, to defacing or downing websites owned by Russian banks and government agencies, to disrupting military supply chain logistics.⁹² Their overall strategic impact on the conflict remains unclear, though it has been reported that they may be integrated into Ukraine’s army reserves in order to acquire legal status.⁹³

4. Pre-Existing Partnerships Make An Enormous Difference

Of all the lessons learned while interviewing for this analysis, the one that most stands out is the importance of building out partnerships and sustaining them—long before any evidence of a crisis breaks.⁹⁴ In particular, interviewees pointed to examples of how relationships cultivated by California National Guard soldiers became a critical foundation for ongoing efforts, instilling trust and a spirit of collaboration between the two countries. In other words, while having a specific task or mission is important, the less tangible value of building a new relationship may be just as valuable when it comes to cybersecurity support abroad.

In other circumstances working relationships had to be created on the fly—yet even these often relied on pre-existing networks. A good example of this came in January 2022, when Microsoft identified an ongoing wiper attack in Ukraine and created a patch for its system. While Microsoft had a commercial office in Ukraine, they did not have the connections to high-level Ukrainian technology officials—and so they reached out to national security officials at the White House to forge a direct partnership. This meant that, when war broke out just a month later, both sides’ leadership knew who to talk to.

In other words, while having a specific task or mission is important, the less tangible value of building a new relationship may be just as valuable.

5. International Cyber Assistance Efforts Remain Early-Stage

On the whole, the fact that so many different U.S. and NATO organizations created special programs or allotted dedicated resourcing to support Ukrainian cybersecurity over the past decade is remarkable. From the Department of the Treasury to private tech companies, and from CISA to CyberCommand, key stakeholders recognized that Ukraine’s cybersecurity directly impacted American security—and that it was important for its own sake. The national security interest for the United States is clear.

Much of the immediate need in Ukraine between 2012 and 2022 was for military and police assistance—areas where USAID, as a development agency, is not positioned to support.

Yet as the phrase “early-stage” implies, some of those cybersecurity assistance efforts were deployed in a sub-optimal manner—whether because of legal or political incompatibilities, the learning curve of deploying a government program for the first time, or the lack of time or resourcing. Most interviewees could point to an initiative that had failed or simply had not been realized in time, such as a U.S. military-supported effort to build a functional virtual training environment for the Ukrainian military.⁹⁵

Interviewees criticized the start-stop nature of some U.S. government programs as making some Ukrainians feel abandoned. They pointed out that organizations like the “Hunt-Forward teams,” for all their successes, aren’t empowered to directly remediate problems. And they argued that

the \$37 million of USAID funding appeared to have had little tangible impact on Ukrainian security, relative to the size of its funding. This is because much of the immediate need in Ukraine between 2012 and 2022 was for military and police assistance—areas where USAID, as a development agency, is not designed to support.⁹⁶

Of course, these are growing pains. “This concept of providing cybersecurity for aid is new,” Goldstein noted.⁹⁷ “We as a country have decades—indeed, in some cases a couple of centuries—of experience providing weapons, providing medical supplies... This idea of providing cybersecurity aid, obviously, by definition is newer. So the mechanisms to provide that aid are being revised as you would expect.”

In the past few years, undoubtedly catalyzed by the ongoing conflict in Ukraine, the U.S. government and private sector have increased their efforts to provide cybersecurity aid abroad. Initiatives that were started just months or years before the outbreak of hostilities are starting to mature. Hunt Forward teams have five years of experience. New authorities and funding—particularly those provided to the U.S. State Department—indicate American commitment to further developing its assistance efforts.

6. Cybersecurity Has No Silver Bullet

For all of the important collaborative work between the U.S. and Ukraine, and for all of Ukraine’s own investments in its digital security, most of those interviewed for this analysis agree that the country’s cybersecurity environment remains underdeveloped. In February 2022, U.S. government officials warned that Ukraine’s power grid was still connected to Russia’s,⁹⁸ and that its digital infrastructure was widely decentralized.⁹⁹ Even as the war has continued, major cyber breaches of public infrastructure have gone undetected, even by companies that spend heavily on cybersecurity.¹⁰⁰ “Rarely have I observed,” one industry leader and former government official told me, “a Ukraine entity that has represented to us that they are operating in what I would consider to be a recognizable enterprise cybersecurity fashion”—that is, one that would be in line with comparable US organizations in the government and private sector.¹⁰¹

Current American officials are quick to convey that this isn’t a critique of Ukrainian leadership, that transforming a country’s cybersecurity posture takes time, and that the COVID pandemic certainly didn’t help. “It is very hard to do cyber at scale in the government,” responded one current Biden Administration cyber leader when asked why the Ukrainians did not modernize and secure their systems more quickly. Another noted that Ukraine’s cybersecurity progress—or lack thereof—was in many ways comparable with other parts of the world. “They’ve mostly followed the path of other countries,” he told me.¹⁰² (Indeed, reports of major cyberattacks and exploitation of American commercial and government networks are common.)

Conclusion

America's ability to effectively provide cybersecurity assistance to allied nations is a national security imperative: in a digitally interconnected world, what happens in one country's network's does not stay there. Ongoing collaboration—in which the United States is ready to learn just as much as teach—is critical in times of both war and peace.

This analysis represents a “first draft” of history—an early effort, despite ongoing limitations on information, to identify what American cyber assistance efforts in Ukraine looked like in the years preceding war, and to endeavor to draw some high-level lessons to guide future programmatic efforts.

It finds that over the past two years of conflict in Ukraine, Ukrainian-American cybersecurity collaboration that long predated the current conflict laid the groundwork for some of the most important success stories of the war. These include the rapid migration of government data to commercial cloud systems—just days before their Ukraine-based servers were destroyed by Russian missiles—and the quick-thinking that ensured that thousands of Starlink terminals could be rolled across the border in a matter of weeks to keep the military—and population—connected. They facilitated the creation of a NATO-standard battlefield situational awareness system, years before the war broke out, that could be revived and deployed rapidly to the field. And they established partnerships and networks of trusted counterparts that could be activated when the crisis broke out.

Still, it is equally apparent that the American experience of providing cybersecurity assistance alongside more traditional methods of development support and military aid remains in the early stages of development. An evaluation of the decade preceding the current outbreak of hostilities in Ukraine paints the picture of an American effort that was simultaneously innovative yet underdeveloped and under-coordinated. Viewed through the lens of the current conflict, it is one in which quick-thinking, luck, and resourcefulness at key moments staved off what could have been a far larger disaster—yet exposed how many opportunities to do more, earlier, were missed.

This analysis represents a “first draft” of history—an early effort, despite ongoing limitations on information, to identify what American cyber assistance efforts in Ukraine looked like in the years preceding war and to endeavor to draw some high-level lessons to guide future programmatic efforts.

Endnotes

- 1 Sharon Rollins, “Defensive Cyber Warfare Lessons from Inside Ukraine,” *U.S. Naval Institute*, June 2023, <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>.
- 2 Tom Balmforth, “Exclusive: Russian hackers were inside Ukraine telecoms giant for months,” *Reuters*, January 2024, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>.
- 3 There is, as to be expected, debate on the severity of Russian cyber attacks and on the mitigating effects of ongoing collaboration efforts. For a detailed analysis, see Jon Bateman, “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications” *Carnegie Endowment for International Peace*, December 2022, <https://carnegieendowment.org/2022/12/16/russia-s-war-time-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657>.
- 4 At the beginning of the war, some watchers were so astonished by what they didn’t see that they speculated that the United States military or intelligence community had stepped in—striking the Russians with their own offensive cyber operations or otherwise using American defensive capabilities to shield Ukraine from cyberattacks. Yet while America’s military cyber operators have alluded to some of their efforts, there is no evidence of a large-scale cyber war being conducted between the United States and Russia. See, e.g. Alexander Martin, “US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command,” *Sky News*, June 1, 2022, <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>.
- 5 Given the timeframes over which cybersecurity improvements are made, the high secrecy surrounding cybersecurity data, the ongoing “fog of war” in Ukraine, and the industry’s lack of standardized metrics for security or security improvements, “appears to have had little impact” does not necessarily mean “had little impact” in the long term.
- 6 David Sanger with Mary Brooks, “New Cold Wars: China’s Rise, Russia’s Invasion, and America’s Struggle to Defend the West,” *Crown*, April 2024, <https://www.penguinrandomhouse.com/books/710053/new-cold-wars-by-david-e-sanger-with-mary-k-brooks>.
- 7 CERT-UA is the Computer Emergency Response Team for Ukraine. It was founded in 2007 and falls under the State Service of Special Communications and Information Protection of Ukraine (SSCIP).
- 8 Nikolay Koval, “Chapter 6: Revolution Hacking,” *Cyber War In Perspective: Russian Aggression Against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Estonia, pg. 55, 2015, https://ccdcoe.org/uploads/2018/10/CyberWarInPerspective_full_book.pdf.
- 9 One major campaign was dubbed “Operation Armageddon.” See Jason Lewis, “Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare,” *Looking Glass Cyber*, n.d. <https://lookingglasscyber.com/blog/threat-intelligence-insights/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/>.
- 10 Mark Clayton, “Ukraine election narrowly avoided ‘wanton destruction’ from hackers,” *The Christian Science Monitor*, June 2014, <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>.
- 11 The relevant clip from the Russian TV segment is shown in the HBO documentary “The Perfect Weapon” (2020).
- 12 See e.g. Natalia Zinets, “Ukraine hit by 6,500 hack attacks, sees Russian ‘cyberwar,’” *Reuters*, December 2016, <https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC>.
- 13 Daniel Brown, “Russian-backed separatists are using terrifying text messages to shock adversaries — and it’s changing the face of warfare,” *Business Insider*, August 2018, <https://www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8>.
- 14 In retrospect, a particularly important conclusion drawn in *Cyber War in Perspective* that should have received more attention is that cyber operations may be less central in a declared shooting war. Instead, they are particularly apt for gray-space operations. (See, “Forward” by Sven Sakkov.) Conceptually, this makes sense: Why craft a delicate and time-consuming cyber operation against a power grid when it could simply be blown irrevocably to pieces? It was a lesson that would come back with full force in 2022.
- 15 Nikolay Koval, “Chapter 6: Revolution Hacking,” pg. 58; and Glib Pakharenko, “Chapter 7: Cyber Operations at Maidan: A First-Hand Account,” pg. 60. *Cyber War In Perspective: Russian Aggression Against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Estonia, 2015.
- 16 Nadiya Kostyuk, “Chapter 13: Ukraine: A Cyber Safe Haven?,” pg. 115. *Cyber War In Perspective: Russian Aggression Against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Estonia, 2015.
- 17 Kostyuk, pg. 114, and Pakharenko, pg. 60.
- 18 Kostyuk, pg. 118.
- 19 Pakharenko, pg. 65.
- 20 Koval, pg. 58.
- 21 The United States’ own systems were permeable to Russian cyber operators, who succeeded in penetrating the networks of the State Department, White House, and Joint Chiefs of Staff over a few months in 2014. Famously, a Chinese state-backed campaign of industrial espionage had been hollowing out the intellectual property of major American companies for years.
- 22 Brian Krebs, “Who’s Selling Credit Cards from Target?” *KrebsOnSecurity*, December 2013, <https://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/>.
- 23 “Sens. Warner, Kirk to Introduce Cybersecurity Amendment to Ukrainian Aid Bill on Monday,” March 2014, <https://www.warner.senate.gov/public/index.cfm/2014/3/sens-warner-kirk-to-introduce-cybersecurity-amendment-to-ukrainian-aid-bill-on-monday>.
- 24 “H.R.4152 - 113th Congress (2013-2014): Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014.” *Congress.gov*, Library of Congress, 3 April 2014, <https://www.congress.gov/bill/113th-congress/house-bill/4152>.

- 25 “Text - H.R.4681—113th Congress (2013-2014): Intelligence Authorization Act for Fiscal Year 2015.” *Congress.gov*, Library of Congress, 19 December 2014, <https://www.congress.gov/bill/113th-congress/house-bill/4681/text>.
- 26 NATO-Ukraine Relations Factsheet, *North Atlantic Treaty Organization*, February 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/220214-factsheet_NATO-Ukraine_Relations_.pdf.
- 27 “FACT SHEET: U.S. and NATO Efforts in Support of NATO Partners, including Georgia, Ukraine, and Moldova,” *The White House*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/09/fact-sheet-us-and-nato-efforts-support-nato-partners-including-georgia>.
- 28 Miruna-Maria Cocolan, “International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence,” *RASIROM*, n.d., <https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf>.
- 29 “NATO’s practical support to Ukraine Factsheet,” *North Atlantic Treaty Organization*, December 2014, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_12/20141202_141202-factsheet-ukraine-suppor.pdf.
- 30 Miruna-Maria Cocolan, “International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence,” *RASIROM*, n.d., <https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf>.
- 31 Original interview. Quoted with permission.
- 32 Original interview. Quoted with permission.
- 33 Alexander Query, “Google opens research and development center in Ukraine,” *Kyiv Post*, January 2020, <https://www.kyivpost.com/post/7682>.
- 34 “Microsoft Ukraine, LLC,” *American Chamber of Commerce in Ukraine*, n.d. <https://chamber.ua/companies/microsoft-ukraine-llc/>.
- 35 See, e.g. Jim Finkle, “Russian hackers target NATO, Ukraine and others: iSight,” *Reuters*, October 2015, <https://www.reuters.com/article/idUSKCN0I308F/>.
- 36 Original interview, conducted on the condition of anonymity.
- 37 The U.S. reportedly targeted the industrial control system of Iran’s nuclear facilities in 2009-2010 (Stuxnet). A series of incidents in 2011 and 2012, attributed to Iran-affiliated hackers, targeted Saudi ARAMCO’s oil production facilities.
- 38 “Cyber-Attack Against Ukrainian Critical Infrastructure,” *Cybersecurity and Infrastructure Security Agency*, last revised July 2021, <https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01>; and “TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *E-ISAC*, March 2016, <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>.
- 39 For a detailed accounting of both the 2015 and 2016 attacks and the American and Ukrainian response, see Andy Greenberg’s “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *WIRED*, June 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
- 40 Joe Slowik, “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack,” *Dragos*, 2019, <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>.
- 41 Original interview. Quoted with permission.
- 42 Original interview. Quoted with permission.
- 43 Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *WIRED*, August 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- 44 Original interview. For a brief overview of some of this work, see “U.S.-Ukraine Energy Cooperation,” *Office of International Affairs, Department of Energy*, n.d., <https://www.energy.gov/ia/us-ukraine-energy-cooperation>.
- 45 “U.S. Support for Connectivity and Cybersecurity in Ukraine,” *Department of State*, May 2022, <https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/>.
- 46 “Cybersecurity Fact Sheet,” *USAID, via ReliefWeb*, May 2022, <https://reliefweb.int/report/ukraine/cybersecurity-fact-sheet>.
- 47 Original Interview.
- 48 “Decree of the President of Ukraine, No. 447/2021,” *President of Ukraine*, August 2021, <https://www.president.gov.ua/documents/4472021-40013>.
- 49 “The United States and Ukraine Hold Third Cyber Dialogue,” *The Department of State*, March 2020, <https://2017-2021.state.gov/the-unity-ed-states-and-ukraine-hold-third-cyber-dialogue/index.html>
- 50 “Opening Remarks by Acting DCM Joseph Pennington at the U.S.-Ukraine Cyber Bilateral Dialogue,” *U.S. Embassy in Ukraine*, March 2020, <https://ua.usembassy.gov/opening-remarks-by-acting-deputy-chief-of-mission-joseph-pennington-at-the-u-s-ukraine-cyber-bilateral-dialogue/>.
- 51 “Administration,” *National Cybersecurity Cluster*, n.d. <https://cybersecuritycluster.org.ua/en/administration/>.
- 52 “The NCCC at the NSDC of Ukraine and CRDF Global host the first session of the National Cybersecurity Cluster,” *National Cybersecurity Cluster*, February 2021, <https://cybersecuritycluster.org.ua/en/news/the-nccc-at-the-nsdc-of-ukraine-and-crdf-global-host-the-first-session-of-the-national-cybersecurity-cluster/>; and “About Cluster,” <https://cybersecuritycluster.org.ua/en/about/>.
- 53 The relevant section of the bills does not appear to have passed in subsequent iterations and was introduced at least once in 2022. “Text - S.814 - 117th Congress (2021-2022): Ukraine Security Partnership Act of 2021.” *Congress.gov*, Library of Congress, 26 April 2021, <https://www.congress.gov/bill/117th-congress/senate-bill/814/text>; and “Text - S.3407 - 117th Congress (2021-2022): Guaranteeing

- Ukrainian Autonomy by Reinforcing its Defense (GUARD) Act of 2021.” [Congress.gov](https://www.congress.gov/bill/117th-congress/senate-bill/3407/text), Library of Congress, 15 December 2021, <https://www.congress.gov/bill/117th-congress/senate-bill/3407/text>; “Text - H.R.6367 - 117th Congress (2021-2022): Guaranteeing Ukrainian Autonomy by Reinforcing its Defense (GUARD) Act of 2022.” [Congress.gov](https://www.congress.gov/bill/117th-congress/house-bill/6367/text), Library of Congress, 1 November 2022, <https://www.congress.gov/bill/117th-congress/house-bill/6367/text>.
- 54 “The United States and Ukraine Hold Third Cyber Dialogue,” The Department of State, March 2020, <https://2017-2021.state.gov/the-united-states-and-ukraine-hold-third-cyber-dialogue/index.html>.
- 55 Original interviews, conducted on background.
- 56 Maj. Mackenzie Deal, “Ukraine’s readiness supported by US Army security assistance experts,” *U.S. Army*, February 2022, https://www.army.mil/article/253753/ukraines_readiness_supported_by_us_army_security_assistance_experts.
- 57 “DOD Announces \$250M to Ukraine,” *U.S. Embassy in Ukraine*, June 2020, <https://ua.usembassy.gov/dod-announces-250m-to-ukraine-2/>
- 58 Jim Garamone, Ukraine-California Ties Show Worth of National Guard Program, *Department of Defense*, March 2022, <https://www.defense.gov/News/News-Stories/Article/Article/2971781/ukraine-california-ties-show-worth-of-national-guard-program/>.
- 59 Original interview, conducted on background.
- 60 Original interview, conducted on background.
- 61 Original interviews.
- 62 “Cybersecurity Fact Sheet,” *USAID, via ReliefWeb*, May 2022, <https://reliefweb.int/report/ukraine/cybersecurity-fact-sheet>.
- 63 “Rising to Ukraine’s Cybersecurity Challenge Through Co-Creation,” *USAID*, n.d. https://2017-2020.usaid.gov/sites/default/files/documents/USAID_UkraineCybersecurityChallenge_CaseStudy_final.pdf.
- 64 “USAID/Ukraine Broad Agency Announcement for Cybersecurity for Critical Infrastructure in Ukraine,” SAM.Gov last updated January 2022, <https://sam.gov/opp/3226e487a347197f206ceda8ca25f65c/view>.
- 65 “Rising to Ukraine’s Cybersecurity Challenge Through Co-Creation,” *USAID*, n.d. https://2017-2020.usaid.gov/sites/default/files/documents/USAID_UkraineCybersecurityChallenge_CaseStudy_final.pdf.
- 66 See, e.g. The USAID Cyber Security for Critical Infrastructure Activity held the first Cybersecurity Dialogue, *The Aspen Institute Kyiv*, September 2022, <https://aspeninstitutekyiv.org/en/proiekt-usaid-kiberbezpeka-krytychno-vazhlyvoi-infrastruktury-ukrainy-proviv-pershyy-dialoh-pro-kiberbezpeku/>.
- 67 Original interviews, conducted on background.
- 68 David Sanger, U.S. Sends Top Security Official to Help NATO Brace for Russian Cyberattacks, *The New York Times*, February 2022, <https://www.nytimes.com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html>.
- 69 Original interview, conducted on background.
- 70 “Defensive Cyber Warfare Lessons from Inside Ukraine,” *U.S. Naval Institute*, June 2023, <https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine>.
- 71 Original interview.
- 72 A more detailed account of how Microsoft responded in early 2022 to the outbreak of war in Ukraine is available in the forthcoming book, *New Cold Wars* (Crown, April 2024).
- 73 Original interview.
- 74 “Destructive malware targeting Ukrainian organizations,” Microsoft Digital Security Unit, January 2022, <https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>.
- 75 Original interview.
- 76 See, e.g. Raphael Satter and James Pearson, “Exclusive: Ukraine prepares potential move of sensitive data to another country - official,” *Reuters*, March 2022, <https://www.reuters.com/world/europe/exclusive-ukraine-prepares-potential-move-sensitive-data-another-country-2022-03-09/>.
- 77 Original interview. See also, Bilyana Lilly on Western cybersecurity assistance to Ukraine,” *CyberScoop*, September 2023, <https://cyberscoop.com/bilyana-lilly-cybersecurity-assistance-ukraine/>.
- 78 Original interview.
- 79 Original interview
- 80 Ulrike Franke and Jenny Soderstrom, “Star tech enterprise: Emerging technologies in Russia’s war on Ukraine,” *European Council on Foreign Relations*, September 2023, <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>.
- 81 Of course, the same risk applies to the political will and staying power of other governments.
- 82 Original Interview.
- 83 Walter Isaacson, “‘How am I in this war?’: The untold story of Elon Musk’s support for Ukraine,” *The Washington Post*, September 2023, <https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/>.
- 84 It is worth pointing out that traditional military contractors like Raytheon or Northrop Grumman would not be expected to provide physical weapons to Ukraine for free. Similarly, digital technology companies in the defense intelligence base, such as Palantir, appear to be directly compensated for their services and products in Ukraine. Meanwhile, commercial companies like Microsoft, Amazon, Google, and other cybersecurity and tech infrastructure companies are not—or at least are less consistently—compensated.
- 85 Walter Isaacson, “‘How am I in this war?’: The untold story of Elon Musk’s support for Ukraine,” *The Washington Post*, September 2023, <https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/>.

- 86 Greg Rattray, Geoff Brown, and Robert Taj Moore, “The Cyber Defense Assistance Imperative: Lessons from Ukraine,” *The Aspen Institute*, February 2023, https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf.
- 87 Original interview.
- 88 For more information on the formation of Aerorozvidka and incorporation into the Ukrainian Armed Forces (and later political struggles within it) see this extended interview. “The army of the future, left in the past. Memoirs of the creator of the disbanded Aerorozvidka,” *Novynarnia*, April 2021, <https://novynarnia.com/2021/04/17/khazin/>.
- 89 Information about the Delta situational awareness system is sourced from original interviews with military representatives and public sources. See e.g. Oscar Rosengren, “Network-centric Warfare in Ukraine: The Delta System,” *Grey Dynamics*, February 2023, <https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/>.
- 90 Original interviews.
- 91 “Hacktivist” is a portmanteau of “hacker” and “activist” and is used to describe an individual who engages in typically criminal computer activity for ideological purposes.
- 92 Janosch Delcker, “Ukraine war: What’s the impact of cyber guerrillas?,” *Deutsche Welle*, December 2023, <https://www.dw.com/en/ukraine-war-whats-the-impact-of-cyber-guerrillas/a-67775539>.
- 93 *ibid.*
- 94 Original interviews.
- 95 Original interview with military source.
- 96 These safeguards preventing crossover between military, police, and civilian organizations is not unique to cybersecurity issues nor is it without justification: they do, however, represent a challenge for the rapid deployment of cybersecurity support.
- 97 Original interview, quoted with permission.
- 98 David Sanger, U.S. Sends Top Security Official to Help NATO Brace for Russian Cyberattacks, *The New York Times*, February 2022, <https://www.nytimes.com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html>.
- 99 Admittedly, while lack of centralized structure makes security controls more difficult to impose, it can also make it easier to build resilience. Attackers must take out multiple companies or networks instead of only a few. See, e.g. Emily Harding, “The Hidden War in Ukraine,” *Center for Strategic and International Studies*, June 2022, <https://www.csis.org/analysis/hidden-war-ukraine>.
- 100 Tom Balmforth, “Exclusive: Russian hackers were inside Ukraine telecoms giant for months,” *Reuters*, January 2024, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>.
- 101 Original interview, conducted on condition of anonymity.
- 102 Original interviews, conducted on background.








**Wilson
Center**






**Science and Technology
Innovation Program**

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

 wilsoncenter.org
 [woodrowwilsoncenter](https://www.facebook.com/woodrowwilsoncenter)
 [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
 [@thewilsoncenter](https://www.instagram.com/thewilsoncenter)
 [The Wilson Center](https://www.linkedin.com/company/the-wilson-center)

Science and Technology Innovation Program

 wilsoncenter.org/science-and-technology-innovation-program
 [@WilsonSTIP](https://twitter.com/WilsonSTIP)
 [linkedin.com/showcase/science-and-technology-innovation-program](https://www.linkedin.com/showcase/science-and-technology-innovation-program)