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

Wilson Center

Science and Technology Innovation Program

Contents

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.

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

Author Notes

—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, .[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.

—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.

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 team[7]—"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]

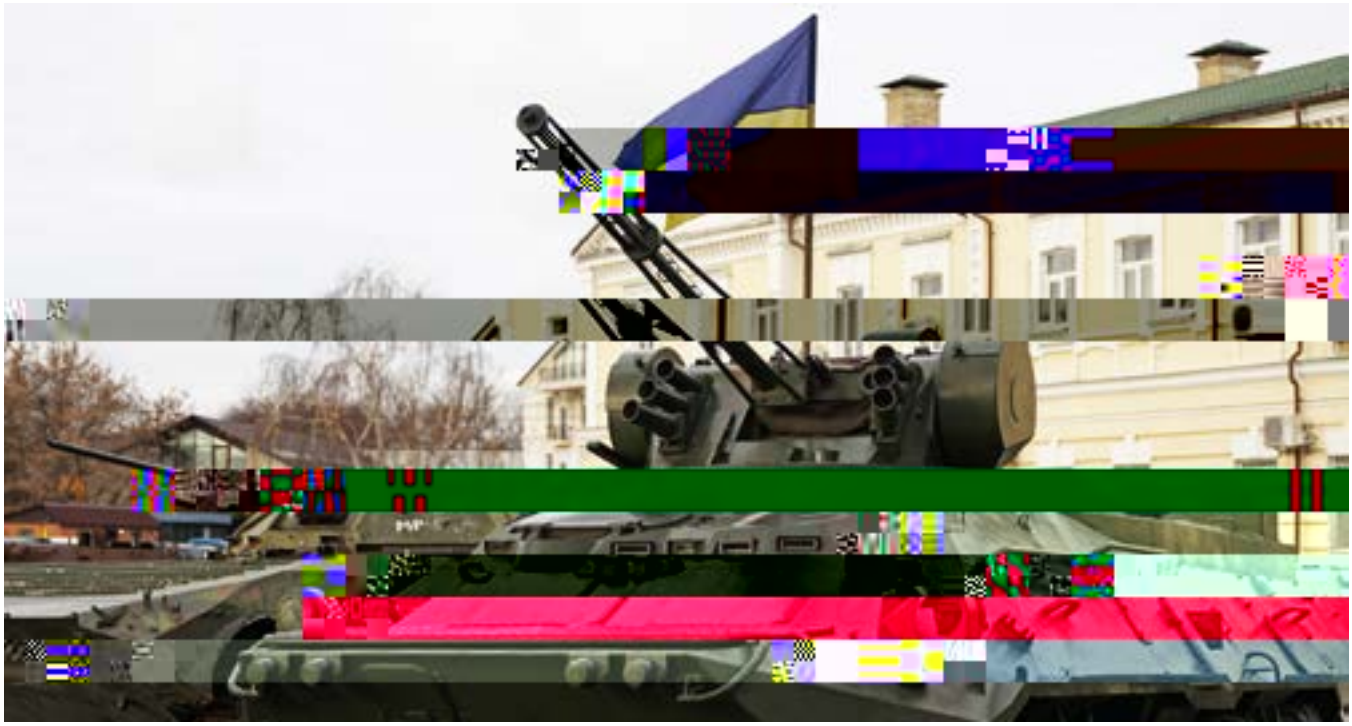
agencies and cells tasked with cybersecurity functions operated autonomously and without a central coordinating structure. Information wasn't shared, and infighting was endemic—sometimes disagreements broke out in front of foreign allies.[18]

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-t of P6): 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]



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

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 E□orts 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 , 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:

> 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.

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]

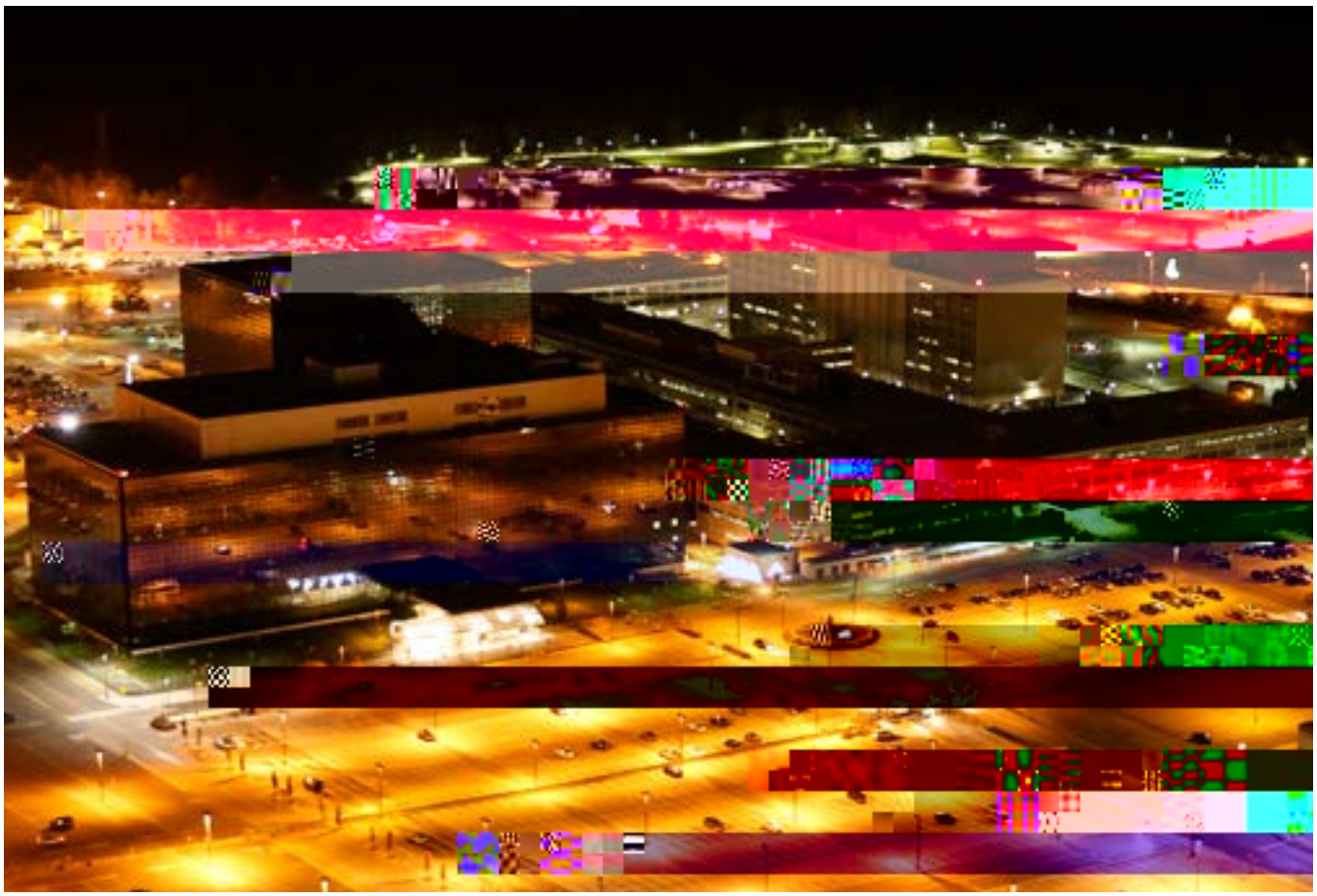
Another category was a combination of **diplomatic and strategic e□orts,** headed by the Department of State. Some of this work supported Ukraine's efforts to rewrite its first national cybersecurity strategy, a task which was conducted by Ukraine's National Security and Defense Council and issued by 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

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.

A , 2013 (0 1.0)



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]

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 hacktivist[91] 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 Di□erence

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

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 rollro allcngs.1 (cia)6.1 (0.(ouS0 (tirc)]TJ0.)17 (aine-)1mkTJ0. t)11 (o g)12 (e epthe molit)- (ar)-14 (y—a]TJ0.013 Tw 0 -1.6 Td[aountrTJ0.atsthat tould bati11 (ed w)henthe cuaoe iou.

Itent t thoeAmerican ce15 (txer)iece ef trevideng tybersecuritaasis4 (ance taong 2 (hsde fmr)17 (e th)17 (aidiion)l cm)12 1 (tihos of Sd)8 (v)8 (el open)10 (t)suportar a aside tn the yaray itange of Sdvel opent 19 . (o. Ad)8 (v)8 (arlu)10 (tion of ghe ydecadepr)17 (eceding whe cur)-7.9 (r)17 (en)10 (

Endnotes

1 Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine," , 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," , 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" , December 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-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,"

25 "Text - H.R.4681—113th Congress (2013-2014): Intelligence Authorization Act for Fiscal Year 2015." , Library of Congress, 19 December 2014, https://www.congress.gov/bill/113th-congress/house-bill/4681/text.

26 NATO-Ukraine Relations Factsheet,

Ce son t