


# CYBER DEFENSE ASSISTANCE AND UKRAINE

**LESSONS AND MOVING FORWARD**



In an era of international instability, the safety and resiliency of our digital existence faces deep challenges. Such instability has undermined the ability of governments to counter aggression in cyberspace. In this growing vacuum, the conduct of cyber defense assistance by the private sector will both change and grow in increasing importance.

In Western and allied nations, the private sector is the dominant producer, operator, and protector of the digital realm. Over the past three years, Western companies have both acted singularly and banded together to provide cyber defense to not only Ukraine in the face of the Russian re-invasion but also to protect the digital environment globally. The need for Western companies to lead in cyber defense and resiliency assistance throughout the international digital environment will likely increase in the years to come. This paper provides lessons to guide these efforts.

# ACKNOWLEDGMENTS

## AUTHORS

**Greg Rattray**  
Executive Director,  
Cyber Defense  
Assistance  
Collaborative (CDAC)

**Seungmin (Helen) Lee**  
Director of Intelligent  
Cyber Research (ICR),  
Next Peak

## CONTRIBUTOR

**Yameen Huq**  
Director, Cybersecurity  
Programs, Aspen Digital

## ASPEN US CYBERSECURITY GROUP

### CO-CHAIRS

**Yvette Clarke**  
U.S. House of  
Representatives

**Christopher Krebs**  
Chief Intelligence &  
Public Policy Officer,  
SentinelOne

**Gary Steele**  
President, Go-to-  
Market, Cisco and GM,  
Splunk

**Kemba Walden**  
President, Paladin  
Global Institute

**Yasmin Green**  
CEO, Jigsaw, Google

### STAFF

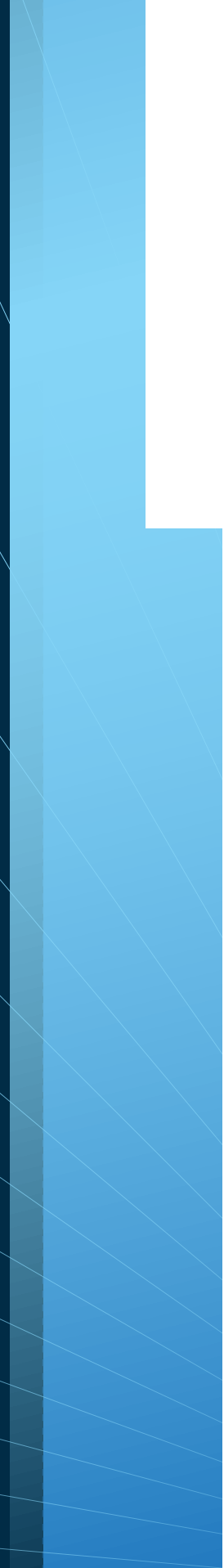
**Yameen Huq**  
Director, Cybersecurity  
Programs, Aspen Digital

**Sasha O'Connell**  
Senior Director,  
Cybersecurity Programs,  
Aspen Digital

**Nicole Tisdale**  
Senior Advisor,  
Cybersecurity Programs,  
Aspen Digital

**John P. Carlin**  
Strategic Advisor and  
Chair Emeritus for  
Cybersecurity, Aspen  
Digital

**Stefani Jones**  
Director, Cybersecurity  
Programs, Aspen Digital



This document was developed in consultation with the Aspen Institute’s US Cybersecurity Group members, who brought forward their ideas and recommendations to Aspen Digital’s cybersecurity policy staff, experts, and advisors. These recommendations would not be possible without their deep public and private sector expertise, which continues to critically challenge how we improve cybersecurity.

### **THE ASPEN INSTITUTE’S U.S. CYBERSECURITY GROUP**

The Aspen Institute’s US Cybersecurity Group is the leading cross-sector, public-private forum for promoting a secure future for America’s institutions, infrastructure, and individuals—in cyberspace and beyond.

# INTRODUCTION

Russia's re-invasion of Ukraine in February 2022 galvanized the West to help resist this aggression. Today, the war continues on many fronts, including cyberspace, but the assistance efforts have slowed as resource constraints and fatigue increasingly set in. Simultaneously, the digital realm in Ukraine continues to be the focus of aggression, both for prosecuting the current conflict as well as a crucial post conflict concern.

In February 2023 the Aspen Institute paper titled "The Cyber Defense Assistance Imperative: Lessons from Ukraine"<sup>1</sup> examined how the private sector established support for Ukrainian cyber defense, discussed its impacts, and derived key lessons from the process. As geopolitical flashpoints near Russia—the Baltic States, Moldova and Poland—and in East Asia—Taiwan and the Philippines—escalate with a substantial cyber component, a deep understanding of future potential challenges to cyber defense assistance (CDA) is crucial. Ukraine's digital resiliency will also be crucial to negotiating and sustaining Ukraine's ability to move beyond the current conflict. Similarly, strong cyber defenses and digital resiliency can improve crisis stability in other potential flashpoints as stated in the U.S. International Cyber Strategy released in May 2024:<sup>2</sup>

**"Public-private partnerships are essential to cyber and digital diplomacy, and they need to be flexible and adaptable. Cyber defense may require new ways to scale, supply, and license cyber defense services and products in a crisis..."**

Today the need for effective, adaptable cyber defense and resiliency bolstered by operational assistance remains essential for Ukraine. The efforts conducted in Ukraine also illuminate how similar geopolitical situations will require similar efforts for achieving the goals for the United States and its allies. This second paper provides an update to our earlier paper and additional findings.

<sup>1</sup> [https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital\\_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf](https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf)

<sup>2</sup> <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/#cyber-attacks>

# EVOLUTION OF THE RUSSO-UKRAINE CONFLICT IN CYBER SPACE

Ukraine's cyber defense remains highly resilient despite an increasing frequency and intensity of Russian cyberattacks. At the end of 2023, Ukraine's largest telecom operator Kyivstar experienced "one of the highest-impact disruptive cyberattacks on Ukrainian networks"<sup>3</sup> since the start of the war.<sup>4</sup> In the first half of 2024, Ukraine experienced 1,739 cyber incidents—a 19% increase from 1,463 cyber incidents in the second half of 2023.<sup>5</sup> At the end of 2024, Russia conducted one of its most severe cyberattacks against Ukraine, targeting Ukraine's state registries and taking them offline.<sup>6</sup> The nature of Russian and Ukrainian cyber operations continues to evolve as well. Ukraine's Computer Emergency Response Team (CERT-UA) announced that Russian cyber operations are focusing on targeting the telecommunication industry<sup>7</sup> as demonstrated by Solntsepek's—Russian state-backed hackers—cyberattacks against Ukrainian internet providers Triacom, Misto TV, Linktelecom, and KIM in March 2024.<sup>8</sup> Throughout 2024 Russia also focused on disinformation campaigns in Ukraine<sup>9</sup> and in Europe<sup>10</sup> to undermine Ukrainian resolve and to deter foreign assistance to Ukraine. Russia also conducted various cyberespionage efforts against organizations directly engaged in the conflict.<sup>11</sup> In response, Ukraine increasingly began adopting a proactive approach, attacking Russian state and private companies to gather intelligence and cause disruptions.<sup>12</sup>

<sup>3</sup> <https://therecord.media/russians-infiltrated-kyivstar-months-before>

<sup>4</sup> The Kyivstar hack is a sophisticated cyberattack, allegedly conducted by Russian state-controlled hacker group Sandworm, against Ukraine's internet infrastructure which resulted in disruption to communications, networks, and connectivity.

<sup>5</sup> <https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report>

<sup>6</sup> <https://www.csoonline.com/article/3629407/russia-fires-its-biggest-cyberweapon-against-ukraine.html>

<sup>7</sup> <https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku%E2%80%8B>

<sup>8</sup> <https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/>

<sup>9</sup> <https://thehill.com/policy/international/4484030-russian-hackers-attack-ukrainian-media-outlets/>

<sup>10</sup> <https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/>

<sup>11</sup> <https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report>

<sup>12</sup> <https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia>

The Ukrainian government is now publicly working with pro-Ukraine hacktivists to target Russian entities: in October 2024 pro-Ukraine hacker group BO Team, which is linked to the Ukrainian military intelligence (HUR), targeted and shut down Russian jurisdiction court websites.<sup>13</sup>

Continued use of cyberattacks by both sides holds the potential for escalation going forward, and the more concerning possibility of Russia escalating cyberattacks against Ukrainian allies, such as Estonia, continues as well. While the focus and severity of Russian disruptive operations have waxed and waned over the past three years, the general trend has been upward and, crucially, the trend may continue even if an accord halts the traditional military conflict.

## PROVISION OF CYBER DEFENSE ASSISTANCE IN UKRAINE TO-DATE

Governments and private sector organizations around the world—though mostly those based in the United States and Europe—have been providing cyber defense assistance (CDA) to Ukraine. Initial efforts proved crucial in assisting Ukraine to fend off distributed denial-of-service (DDoS) attacks, establishing resilient cloud-based digital services, gaining situational awareness of Russian cyberattacks across the Ukrainian attack surface, and hunting to remove Russian intrusions into networks. The Cyber Defense Assistance Collaborative (CDAC)<sup>14</sup> as well as other private sector companies made focused efforts to provide the Ukrainian organizations the specific assistance requested to meet the urgency of the situation and build trust. However, concerns about the longer-term efficacy and sustainability of certain activities continued as these efforts began to scale up.

In the public sphere, the U.S. government delivered more than \$82 million in cyber assistance to Ukraine between February 2022 and August 2024,<sup>15</sup> but cyber assistance programs have often been broadly targeted and include a focus on the post-conflict

<sup>13</sup> <https://therecord.media/russian-court-websites-down-attack-claimed-pro-ukraine-group>

<sup>14</sup> <https://crdfglobal-cdac.org/>

<sup>15</sup> <https://www.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue/#:~:text=As%20part%20of%20this%20support,over%20%24120%20million%20since%202016>. The source has been archived, current as of Jan 22, 2025, but was available in August 2024.

recovery.<sup>16</sup> The U.S. government also continues to face a growing partisan divide regarding its support for Ukraine<sup>17</sup> as well as conflicting priorities in terms of how it focuses its assistance and global geopolitical commitments. Additionally, while it is currently unclear how the new Trump administration will affect prospects for cyber defense assistance to Ukraine, President Trump did freeze all foreign aid for 90 days as of January 21, 2025. The continuation of private sector assistance through CDAC and other efforts persists as of the time of this report.

Internationally, individual nations continue to support Ukraine's cyber defenses as well. For example, the United Kingdom expanded its CDA to Ukraine in June 2023 by 16 million Euros and two years.<sup>18</sup> Moreover, like-minded nations are coming together to establish formal mechanisms to support Ukrainian cyber defense such as the following:

- **Tallinn Mechanism:**<sup>19</sup> The United States, Canada, Denmark, Estonia, France, Germany, the Netherlands, Poland, Sweden, and the United Kingdom formalized the Mechanism in December 2023 with the Ukrainian government to coordinate and facilitate non-military cyber defense capacity building assistance, focused on critical infrastructure. The Mechanism seeks a singular, prioritized set of Ukrainian national cyber assistance requirements, but Western donor nations will coordinate individual national assistance efforts. As the Mechanism evolves, dialogue regarding how to orchestrate private sector involvement and deploy advanced cyber defense capabilities in a timely fashion continues. On December 20, 2024, the Tallinn Mechanism published a joint statement, commemorating the anniversary of the Mechanism and highlighting that the Mechanism collected over 200 million euros in foreign aid assistance. The Mechanism also mentioned that it "will continue to seek new avenues for supporting Ukraine for as long as it takes."<sup>20</sup>

<sup>16</sup> <https://therecord.media/us-cyber-ambassador-fick-cyber-aid-to-ukraine-kyiv>

<sup>17</sup> <https://www.pewresearch.org/global/2024/05/08/growing-partisan-divisions-over-nato-and-ukraine/>

<sup>18</sup> <https://www.gov.uk/government/news/uk-to-give-ukraine-major-boost-to-mount-counteroffensive>

<sup>19</sup> <https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/>

<sup>20</sup> <https://vm.ee/en/news/joint-statement-tallinn-mechanism>



- **IT Coalition:**<sup>21</sup> Ten European nations including Estonia, Luxembourg, Belgium, Denmark, Iceland, Italy, Latvia, Lithuania, and the Netherlands formalized the Coalition in February 2024 to support Ukraine's Defense Ministry and Armed Forces' Information Technology (IT) infrastructure for the next six years. The Coalition's efforts encompass the full range of Ukrainian military IT and communications needs. In May 2024 the IT Coalition delivered communications hardware to Ukraine and confirmed a new contribution of 22 million euros from Luxembourg, Iceland, Estonia, and Belgium.<sup>22</sup> The United States has been an observer of the Coalition's activities but has not formally joined.

The emergence of the Tallinn Mechanism illuminates both challenges and opportunities faced by government-led CDA. The Mechanism has proved effective in motivating the establishment of a coordinated set of Ukrainian cyber defense requirements. However, initial discussions regarding the Tallinn Mechanism began in early 2023. The slow pace of the launch and orchestrating commitments from participating governments stems from the traditional deliberate process of multilateral diplomacy. Similar delays in contracting processes may well plague efforts to integrate the private sector into the provision of strategically impactful assistance.

Many sources of CDA exist in the private sector with varying degrees of coordination between companies and governments involved. CDAC continued to coordinate assistance to Ukraine and has helped deliver over \$40 million in assistance, including over 2,600 instances of cyber defense tools and more than 1,600 training credits or sessions, to 25 Ukrainian entities from 32 private sector companies.<sup>23</sup> Outside of CDAC, Microsoft and other cloud-based services provisioned digital services as Russia bombed Ukrainian data centers and power grids;<sup>24</sup> Cloudflare provided counter DDoS services as Russia used relatively unsophisticated DDOS attacks to suppress digital government, banking, and telecommunications services.<sup>25</sup>

<sup>21</sup> <https://kyivindependent.com/it-coalition-members-sign-cooperation-agreement-in-support-of-ukraine/>

<sup>22</sup> <https://www.mil.gov.ua/en/news/2024/05/31/the-it-coalition-led/>

<sup>23</sup> CDAC internal tracker current as of October 23, 2024.

<sup>24</sup> <https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/>

<sup>25</sup> <https://blog.cloudflare.com/ukraine-update>

Many governments have contracted private sector entities to provide a wide range of cyber capabilities and conduct incident response and hunting operations.

CDAC's groundbreaking efforts to provide operational capabilities began within weeks of the conflict's start. In particular, CDAC members provide attack surface monitoring and threat intelligence sharing through its members and a custom threat intelligence platform.<sup>26</sup> Early CDAC intelligence support efforts in 2022 gave Ukrainian organizations—such as State Special Communications Service of Ukraine (SSSCIP), SBU, and National Cybersecurity Cluster (NCCC)—daily attack surface monitoring and specific Russian threat and attack characteristic feeds, bolstering their ability to both defend against and quickly recover from attacks. By the end of 2023, Recorded Future provided over \$10 million in intelligence data, Intelligence Cloud software platform, and Russian war crimes investigation to Ukraine, especially Ukrainian critical infrastructure. The company delivered an additional 13 million in 2024.<sup>27</sup> By collaborating with its partners—ThreatQuotient, Recorded Future, Mandiant (part of Google Cloud), and the Cyber Threat Alliance (CTA)—CDAC has further developed a centralized aggregator and distributor of threat intelligence that de-duplicates and prioritizes intelligence for a range of Ukrainian government and private sector recipients. The platform is a hallmark of public-private partnership as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides its feed to the platform along with private sector companies as described below:

**“CISA continues to urgently support our Ukrainian partners and provide all possible information and services to advance their cyber defense,” said CISA Associate Director Clayton Romans. “By working with key partners like CDAC, we are able to catalyze information sharing and help bring the best capabilities of government and industry to support Ukraine during this challenging time.”**

CDAC participants have strengthened Ukraine's longer-term cyber defense capability as well. Key tools include Security Information and Event Management (SIEM) systems, End

<sup>26</sup> <https://crdfglobal-cdac.org/case-study-threat-intelligence-sharing/>

<sup>27</sup> <https://www.recordedfuture.com/press-releases/recorded-future-continues-provide-intelligence-ukraine>

Detection Response (EDR) tooling, and vulnerability scanners. The SANS Institute has been developing and sharing resources to build the necessary human capital by providing cyber training and education to Ukraine.<sup>28</sup>

Beyond assistance delivery, CDAC has built a strong community that can effectively mobilize and address strategic and operational challenges in cyberspace by being a model for collaborative organization and provide tools, services and training that can be integrated into other mechanisms such as the Tallinn Mechanism and the IT Coalition. Through on-going CDAC meetings and quarterly convenings of its over 50 private and government participants, CDAC provides a unique forum for exchanging information on cyber defense initiatives and for sustaining trust that allows a vigorous dialogue about what is working and what challenges exist.

In the first half of 2024, CDAC, in conjunction with Columbia University School of International and Public Affairs, created a novel framework for measuring the CDA effectiveness. The framework—based on relevant open-source research, a review of existing evaluation frameworks, and expert interviews—proposes a three-phased approach for evaluating the operational, strategic, and organizational effectiveness of CDA. The phased approach allows for measurement of effectiveness at different points of a conflict. The approach is also comprised of five key pillars—operational success, efficiency, strategic planning, friction, and sustainability—that can help participants better target their assistance and address concerns regarding program effectiveness expressed by potential CDA funders.<sup>29</sup>

Despite the progress made and the new mechanisms established, barriers to receiving prioritized CDA requests and feedback on the effectiveness of assistance continue to exist. Since the inception of the conflict, many Ukrainian organizations have sought assistance from an overlapping set of donors, sometimes providing conflicting lists of requests to different organizations. Also, continuing changes at all leadership levels within Ukrainian organizations have slowed coordination of the assistance and increased hesitancy of donors. CDAC's Blue Force Tracking, Assessment, and Coordination effort has gained the interest of public and private sector providers but remains unfunded,

<sup>28</sup> <https://www.sans.org/blog/ukraine-russia-conflict-cyber-resource-center/>

<sup>29</sup> <https://crdfglobal-cdac.org/cda-evaluation-framework/>

anemic, and gathers information in an ad-hoc fashion. As the conflict has lasted beyond the envisaged timeframes, licenses and training that were originally envisaged as one-time actions continue to require sustainment and renewals. Dialogues with governments about structured long-term sustainment of these efforts have progressed slowly despite the situation in Ukraine.

While CDAC and other private sector efforts have been more openly acknowledged and praised as the conflict progressed, tracking the provision and effectiveness of such assistance and the measurement of its effectiveness remains difficult. Cyber assistance providers can be reluctant to share specific information on the assistance that they have delivered for various reasons: contractual arrangements, corporate security concerns, and public awareness of involvement in the conflict. Recipients often do not have the time or capability to provide feedback of the assistance's impact. Reporting and data collection necessary for measuring CDA effectiveness requires resources and planning.<sup>30</sup>

Based on observations in early 2025, the private sector is largely sustaining capabilities provided through early CDA activities including intelligence support, software licenses, training programs and other assistance. However, the level of new requests and initiatives has diminished significantly. Various factors are influencing this situation including 1) successful Ukrainian digital resilience, 2) perceptions of Russian cyber ineffectiveness in the cyber domain, 3) fatigue among certain assistance providers, 4) lack of dedicated funding to support large-scale, systemic initiatives, and 5) uncertain impacts of assistance efforts.<sup>31</sup> Different perspectives exist regarding whether digital and cyber assistance to Ukraine should be focused on addressing short-term cyber defense gaps or longer-term digital resilience. Coherence around the right priorities and coordination of efforts remains largely aspirational.

<sup>30</sup> <https://crdfglobal-cdac.org/cda-evaluation-framework/>

<sup>31</sup> CDAC Blue Force Tracker and operations

# LESSONS LEARNED AND FUTURE EFFORTS

The Russia-Ukraine War has provided several lessons for future CDA initiatives. The first Aspen paper highlighted three primary lessons: 1) the need to establish early connections and trust between CDA recipients and providers; 2) the need to identify, assemble, and organize capability providers; 3) the need to align activities and priorities when it comes to CDA. These lessons have continued to hold true since that paper was published, and CDA providers are still working to fully incorporate these lessons into policies and actions. On the positive side, strong trust exists between a large set of Ukrainian recipients and Western nations and companies providing assistance. Such trust was built largely by meeting Ukrainian requests and learning to work with them to deliver information and technology in an on-going and maturing fashion. The Tallinn Mechanism, the IT Coalition, and CDAC continue to provide venues for organizing capability providers even though alignment of priorities continues to face challenges.

Beyond these initial findings, the hard-won experience of delivering CDA in Ukraine over the past two and a half years of conflict has resulted in at least five additional lessons:

## **1) SEEK TO ESTABLISH A TRANSPARENT AND PRIORITIZED LIST OF REQUIREMENTS AND COORDINATED DELIVERY.**

The recipient nation will likely be best served when it develops a consolidated and prioritized list of requirements for potential providers because this helps align activities and establish priorities. Establishing national cyber priorities is difficult in any circumstance, so such efforts should focus practically on identifying the assistance of most impact to the most crucial national assets at the highest risk. At times this goal may be difficult to meet based on the nature of the recipient's political structure, cyber maturity, or the presence of a conflict or an emergency. In Ukraine the urgency of the early phase of the conflict made this impossible. This finding argues for conducting such assessments prior to the onset of kinetic conflict to the extent possible. Ukraine also found this consolidation difficult due to the lack of capability in conducting self-assessments that would generate the prioritized list of requirements; thus, CDA can usefully include provision of assessment services to properly understand needs. The Tallinn Mechanism has helped provide the right incentives for such

prioritized requirements as well as the ability to aggregate resources at a level to seek strategic impact. Furthermore, having situational awareness regarding previously delivered assistance can help avoid duplication and inefficiency as well as allow for a deeper understanding regarding which assistance is effective. However, sensitivity of both donors and recipients regarding the presence, focus and effectiveness of the activities, and decentralized delivery of assistance create barriers to situational awareness.

## **2) ENSURE WESTERN GOVERNMENTS ESTABLISH CONTINUED FUNDING MECHANISMS FOR ACCELERATED CDA.**

Due to the lack of precedent in providing CDA that heavily involves the private sector, formal mechanisms to identify, support, and channel CDA distinct from longer-term cyber capacity building efforts did not exist in the United States before the Russia-Ukraine War. Formal mechanisms began organizing in late 2023—nearly two years into the conflict. The lack of funding mechanisms and the sense that the immediate crisis has passed led to an atrophy of voluntary assistance by the private sector. Furthermore, CDA to Ukraine has been deprioritized against potential new conflicts and now is impacted by domestic politics. A long-term, dedicated funding mechanism for CDA activities would help reduce this variability. Furthermore, the long-term dedicated funding should focus on supporting global stability, delivering cost-efficient CDA, and providing sectoral-level improvements to the recipient nation.

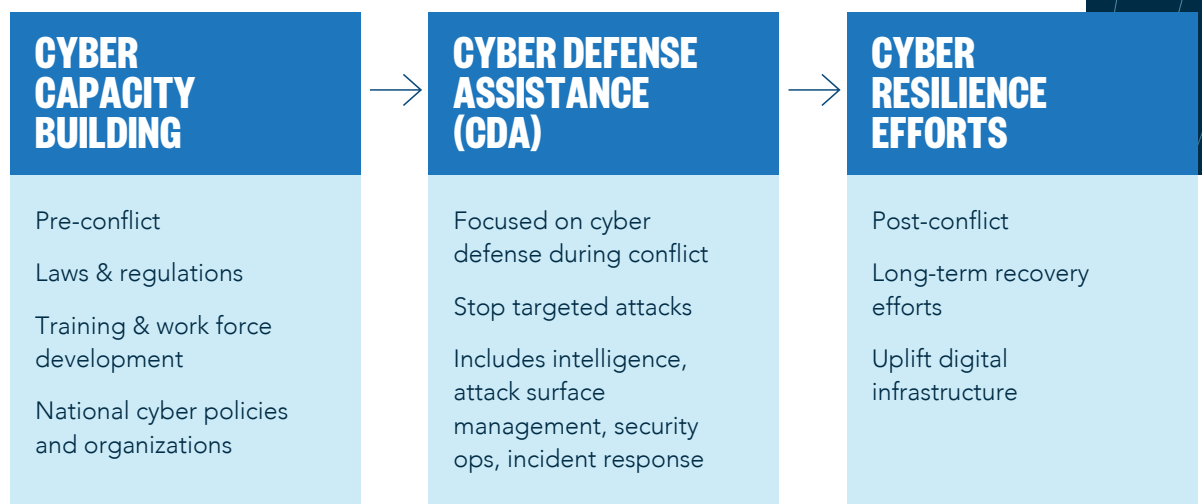
## **3) SHARPEN CDA CAPABILITIES TO PROVIDE SITUATIONAL AWARENESS AND INTELLIGENCE TOOLS.**

CDAC has delivered various tools and services that help provide situational awareness and intelligence tools such as attack surface monitoring by Looking Glass—now Zero Fox—and ThreatQuotient and Recorded Future’s intelligence platforms. Christopher Day, Vice President of Strategic Capabilities and Programs and Deputy Chief Technology Officer (CTO) of Tenable, explains it well:

“Visibility is important to a defender. By visibility I mean technical cyber telemetry collected from and about your operating environment as well as intelligence about your adversary. It is difficult to stop an attacker you know nothing about or can’t see operating against your systems. Specifically, the bright light that Western government and commercial intelligence providers shined on Ukraine made it very difficult for Russia to conduct offensive cyber operations against Ukrainian networks and systems.”

#### 4) DIFFERENTIATE AMONG CYBER CAPACITY BUILDING, CDA, AND CYBER RESILIENCE FOR RESOURCE PURPOSES.

Due to overlapping sets of activities, clear divisions between types of cybersecurity assistance are somewhat arbitrary. However, distinguishing between cyber capacity building, CDA, and cyber resilience is useful for resource allocation decisions, and associated timing and priorities. Cyber capacity building generally involves laws and regulations, training and work force development, and helping to ensure that effective national cyber policies and organizations are in place before a conflict occurs. CDA refers to helping governments and critical infrastructure organizations with the ability to stop targeted attacks, including activities such as incident response and attack surface monitoring. Cyber resilience is a long-term movement to uplift the digital infrastructure—such as the cloud—supporting governments and critical infrastructure.



These activities exist along a spectrum, and defending a nation in cyberspace requires efforts along the entire continuum at the right time. Therefore, policy makers and the cybersecurity industry should develop definitions for these categories of assistance that can help ensure balanced packages for recipient nations.

## **5) ESTABLISH FOCUSED OPERATIONAL LINES OF EFFORT TO PRE-POSITION AND PREPARE FOR CONFLICTS.**

The 2023 Aspen Institute paper on CDA<sup>32</sup> highlighted the need to establish early connections and trust between recipients and providers as well as the need to identify, assemble, and organize capability providers. Recipients and providers need to go one step further to prepare in advance for potential conflicts by collaborating on tabletop exercises, red team efforts, security operation center (SOC) uplifts, and other operational work to develop the capability to defend against cyber operations amid conventional conflicts. To be effective, such preparations require engagement from stakeholders combined with a coordination hub to focus, plan and execute the activities. An organization such as CDAC could orchestrate such activities by bringing in member companies, potential recipients and government organizations, if appropriately resourced.

## **POTENTIAL FUTURE APPLICATIONS**

Although the outcomes and timing remain uncertain in Ukraine, the Baltics, Moldova, or Poland may become Russia's next target for focused aggression. Moldova is a small country between Ukraine and Romania and has historic ties to Russia. Even as Russia is waging war against Ukraine, it is conducting cyber operations in Moldova to destabilize pro-Western President Maia Sandu's regime.<sup>33</sup> The Baltics are in a similar situation and mirror Estonia's situation from 2007.<sup>34</sup> At the beginning of the year, Aleksey Zhuravlyov—a Russian lawmaker and member of the State Duma—suggested that Poland, along with other previous Soviet Union territories, may be Russia's next target as well.<sup>35</sup>

<sup>32</sup> [https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital\\_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf](https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf)

<sup>33</sup> <https://www.csis.org/analysis/moldovas-fate-tied-ukraines-now-time-west-go-big-moldova>

<sup>34</sup> <https://www.nytimes.com/2007/05/29/technology/29estonia.html>

<sup>35</sup> <https://www.newsweek.com/putin-ally-says-poland-next-ukraine-war-rant-russian-tv-1860470>



In May 2024, Poland's CERT (CERT-PL) commented that hacker group APT28, associated with Russia's military intelligence agency (GRU), targeted Poland with a widespread espionage and malware campaign.<sup>36</sup> These nations face similar threats as Ukraine and may face increasing cyberattacks as the situation in Ukraine continues to evolve. The cyber defense community and organizational fabric being developed for Ukraine can be leveraged in the Baltics, Moldova and Poland as well.

Geopolitical tensions in East Asia are also increasing. At the end of last year, Chinese President Xi Jinping publicly declared his intentions to reunify China with Taiwan in the future although he did not agree with the publicized timeline of 2027.<sup>37</sup> If tensions were to escalate in the Taiwan Strait, most analysts predict China will use cyberattacks to coerce Taiwan<sup>38</sup> or to hinder allies' assistance. Taiwan experienced more than 2.4 million cyberattack attempts per day, which is twice as many as the 1.2 million daily average in 2023.<sup>39</sup> Chinese efforts to conduct cyberespionage and disruptions also increased in the United States the 2024 Salt Typhoon campaign that affected at least nine U.S. telecommunication companies<sup>40</sup> and has been explicitly acknowledged by Australia<sup>41</sup> and Japan.<sup>42</sup> China has also been increasing its misinformation and hacking campaigns against the Philippines.<sup>43</sup> While the existing cyber defense community can be leveraged in a potential Taiwan Strait crisis, some experts are concerned that U.S. companies' economic relations with China would hinder the U.S. private sector from supporting Taiwan.<sup>44</sup> However, many Western technology and cybersecurity companies such as those in CDAC have already cut most ties with China and many are involved in helping Taiwan. The possibility of engaging the private sectors in allies already impacted such as Australia and Japan also exists.

<sup>36</sup> <https://therecord.media/poland-cyber-espionage-russia-gru>

<sup>37</sup> <https://www.nbcnews.com/news/china/xi-warned-biden-summit-beijing-will-reunify-taiwan-china-rcna130087>

<sup>38</sup> <https://thediplomat.com/2024/02/in-a-crisis-could-china-coerce-taiwan-through-cyberspace/>

<sup>39</sup> <https://www.darkreading.com/cyber-risk/as-tensions-with-china-mount-taiwan-sees-surge-in-cyberattacks>

<sup>40</sup> <https://www.darkreading.com/cyberattacks-data-breaches/china-salt-typhoon-charter-windstream-telecom-victims>

<sup>41</sup> <https://itwire.com/guest-articles/guest-opinion/a-wake-up-call-for-australia%E2%80%99s-telecom-sector-lessons-from-the-u-s-salt-typhoon-hack.html>

<sup>42</sup> <https://www.asahi.com/ajw/articles/15570789>

<sup>43</sup> <https://www.darkreading.com/cyberattacks-data-breaches/philippines-pummeled-by-assortment-of-cyberattacks-tied-to-china>

<sup>44</sup> <https://cset.georgetown.edu/publication/which-ties-will-bind/>

## CONCLUSION

The importance of private sector-led cyber assistance and cyber defense in future conflicts is evident. The last three years of conflict in Ukraine led to new mechanisms and organizations that helped coordinate cyber defense assistance. The evolution of CDA activities in Ukraine also demonstrated the need for transparent, prioritized requirements from the recipient nation, the importance of establishing dedicated, long-term funding mechanisms, the value of operationally focused assistance, and the need to pre-position lines of efforts to prepare for conflicts. As geopolitical tensions around Russia and in East Asia continue to demonstrate a growing cyber component, these lessons are crucial to help the US manage crises and, if needed, successfully defend its allies and friends.

# COPYRIGHT © 2025 BY THE ASPEN INSTITUTE

This work is licensed under the Creative Commons Attribution Noncommercial 4.0 International License.

To view a copy of this license, visit:

<https://creativecommons.org/licenses/by-nc/4.0/>

Individuals are encouraged to cite this report and its contents. In doing so, please include the following attribution:

“Cyber Defense Assistance and Ukraine.” Aspen Digital, a program of the Aspen Institute, March 2025. CC BY-NC.  
[www.aspendigital.org/report/cyber-defense-assistance-ukraine](http://www.aspendigital.org/report/cyber-defense-assistance-ukraine).