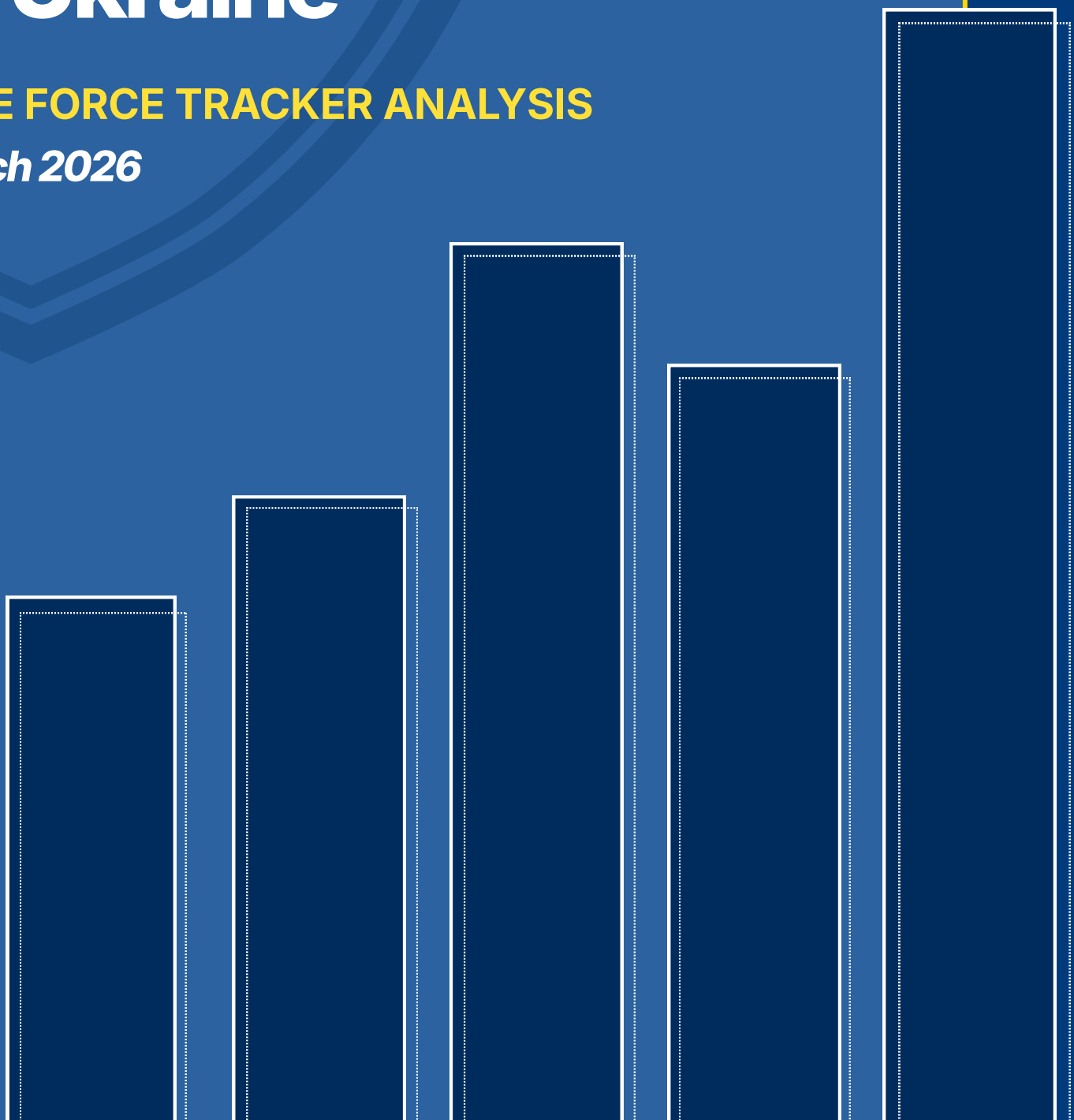
CDAC
A CRDF GLOBAL INITIATIVE

Four Years of Cyber Assistance to Ukraine

BLUE FORCE TRACKER ANALYSIS

March 2026



CONTRIBUTORS

Project Lead	Seungmin Helen Lee
Author	Yevheniia Yefymova
Visual Designer	Jordan Paik
Date	March 2026

ABOUT CDAC

Cyber Defense Assistance Collaborative

The Cyber Defense Assistance Collaborative (CDAC) is a consortium of leading cybersecurity companies, former US government officials, and top US cyber defense leaders who came together to provide operational cyber defense assistance tor Ukraine since the 2022 Russian full-scale invasion of Ukraine. Between 2022 and 2025, CDAC has delivered nearly USD 50M worth of assistance which includes over 2,600 cyber defense tools and over 1,800 training credits and sessions. CDAC also houses the Blue Force Tracker initiative which has been recording and analyzing cyber defense assistance delivered to Ukraine since February 2022.

TABLE OF CONTENTS

Section 1. Introduction

Since the start of Russia's full-scale invasion in 2022, Ukraine has faced a sustained and evolving wave of cyberattacks aimed at disrupting critical state functions and undermining societal resilience. Russian cyber actors have consistently sought to identify and exploit the digital sphere alongside conventional military strikes as part of a broader strategy designed to weaken Ukraine's capacity to govern and sustain its war effort.[1]

After four years of full-scale war, governments, private-sector actors, and research institutions are increasingly attempting to distill lessons from Ukraine's experience to inform future models of cyber defense assistance (CDA). This report analyzes the CDA provided to Ukraine by foreign governments, the private sector, and coordination mechanisms to better understand the CDA delivery process and structure.

The outcomes of this paper reveal the following:

1. Foreign government CDA and private-sector CDA differ in various aspects: the size of CDA delivery, the speed of mobilization and implementation, and the types of assistance delivered.
2. Coordination mechanisms could allow for more visibility and efficiency but also have been prone to administrative friction and a lack of consistent transparency practices.
3. Hardware remains a high priority, but an emerging focus on training could signal a shift towards longer-term resilience and domestic capabilities.

1. Maksym Beznosiuk and William Dixon, "Saving Ukraine's Power Grid," CEPA, February 13, 2026, https://cepa.org/article/saving-ukraines-power-grid/.

Section 2. Methodology & Limitations

This report's analysis draws on the Cyber Defense Assistance Collaborative's (CDAC)[2] Blue Force Tracker (BFT) effort which has been systematically recording cyber defense assistance (CDA) delivered by public and private-sector organizations since CDAC's establishment in 2022. The BFT draws from three categories of sources: open-source research; recorded CDA delivery through CDAC's coordination; and conversations and discussions between CDAC and relevant stakeholders.

The open-source research includes news articles, company blogs and announcements, government websites, think tank reports and more. The record of CDAC's deliveries includes non-publicly disclosed information—such as recipient organization name, provider organization name, exact description of CDA delivered—that the CDAC stakeholders have voted to anonymize in a public-facing report. At times, discussions also needed to be anonymized. When available, a public-facing source was cited to further support this paper's data and analysis.

This report analyzes all available BFT dataset from the beginning of the war in February 2022 through the end of 2025. CDA efforts that began before the war but endured into the February 2022 - December 2025 were excluded from the analysis. The monetary values in foreign currencies were standardized to USD using annual average exchange rates for the relevant calendar year (local currency units per USD). The BFT dataset used for this report's figures and analysis is available separately on the CDAC website.

Several limitations resulting from limited available data and data quality exist. First, not all delivered or committed CDA are recorded or known. Thus, it is likely that the actual delivered and committed CDA to Ukraine exceeds the values in this report.

2. Cyber Defense Assistance Collaborative (CDAC), 2022, https://crdfglobal-cdac.org/.

Second, the specificity of a CDA datapoint (i.e., assistance value, aid specifics, recipient identification, etc.) tends to differ across the data set. Many providers deliberately avoid disaggregating CDA data to protect their own branding and operations, Ukraine's operational and technological advantages, the security of implementing agencies, and sensitive supply chain relationships.

At times, the lack of transparency created uncertainties regarding whether a CDA data point could be accounted for twice. In these cases, the report errs on the conservative side and has excluded such data points from the graphics and analysis.

Third, the report acknowledges that the actual date of CDA delivery could not be adequately captured because recording or public announcements of CDA delivery tend to lag behind the actual delivery date.

Finally, this report excludes certain memorandums, agreements, and bulk aid packages that reference Ukraine, where the available information is insufficient to determine the precise nature or specific value of CDA delivered. The excluded information includes:

1. Agreements that lack a clearly associated value or confirmed delivery (i.e., Agreement on security cooperation and long-term support between Ukraine and the Federal Republic of Germany)[3]
2. Bulk packages covering multiple recipient nations without specifying Ukraine's allocated share (i.e, 2019-2023 Action on Cybercrime for Cyber Resilience for Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine)[4]
3. Broader assistance packages that bundle CDA with humanitarian, educational, or other forms of aid without disaggregating the components (i.e., 2024 Assistance captured in the Agreement on Security Cooperation between Canada and Ukraine).[5]

---

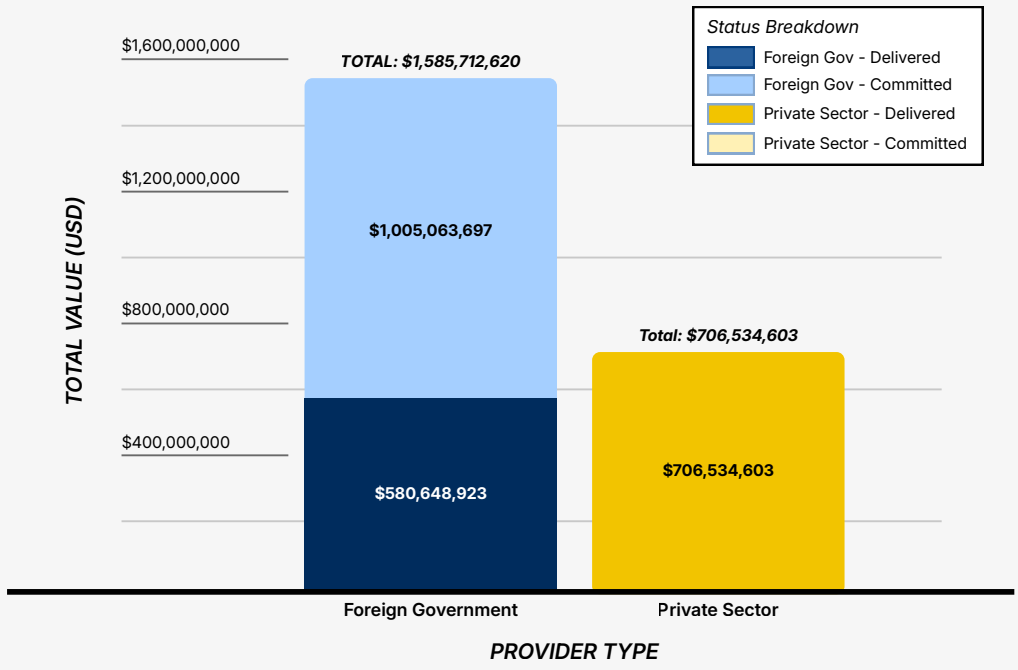
3. Volodymyr Zelenskyy, "Agreement on Security Cooperation and Long-Term Support between Ukraine and the Federal Republic of Germany," Official website of the President of Ukraine, February 16, 2024, https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-88985.
4. CyberEast+, Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region, March 2025, https://rm.coe.int/2088-cybereast-summary-and-workplan-december-2022/1680aa0773.
5. "Canada Announces Additional Support for Ukraine," Prime Minister of Canada, February 24, 2024, https://www.pm.gc.ca/en/news/backgrounders/2024/02/24/canada-announces-additional-support-ukraine

Section 3. Overview of Cyber Defense Assistance (CDA)

Over the last four years, various types of actors have emerged in the donor or provider community, shaping the Ukraine's cyber defense ecosystem. Largely, donor types include foreign governments, private-sector companies, and coordination mechanisms. Appendix 1 includes a sample chart of this donor community.

Figure 1 below visualizes the disclosed overall CDA by provider type and status of delivery. The different status of delivery included delivered or implemented and pledged or committed. More specifically, the second status category indicates that the CDA has not yet been delivered.

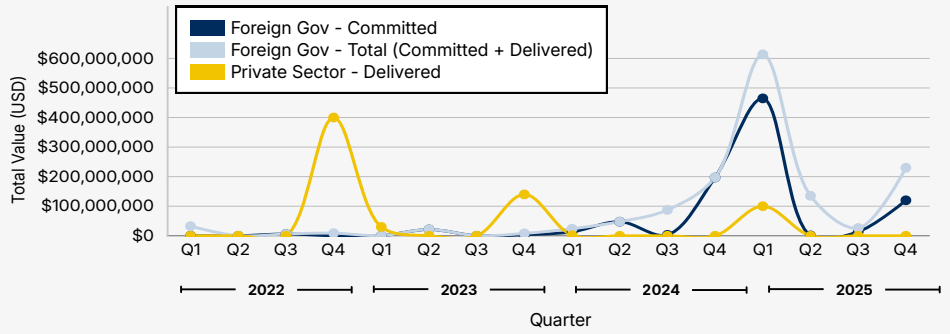
Figure 1. Overall Disclosed CDA (USD)



Source: CDAC BFT Dataset released March 4, 2026

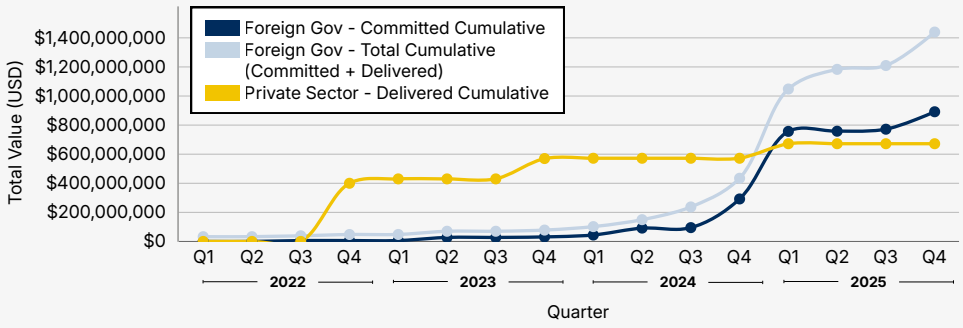
The dataset leveraged in this report captures approximately USD 2.29B in delivered and committed CDA and USD 1.29B delivered. The captured CDA reflects a mixed economy of assistance from high-value government packages to high-volume but low-value operational private-sector assistance. As a comparison, international military aid to Ukraine since February 2022 totals USD 190.7B,[6] making CDA only around 1.2% of that figure. Figure 2 below illustrates the quarterly evolution of CDA to Ukraine, distinguishing between provider type and status of delivery, and Figure 3 represents the same data but cumulative over each quarter.

Figure 2. Foreign Government & Private-Sector CDA by Quarter (USD)



Source: CDAC BFT Dataset released March 4, 2026

Figure 3. Cumulative CDA by Quarter (USD)



Source: CDAC BFT Dataset released March 4, 2026

6. Antezza, A., Bomprezzi, P., Bushnell, K., Dyussimbinov, Y., Frank, A., Frank, P., Franz, L., Kharitonov, I., Kumar, B., Nishikawa, T., Rebinskaya, E., Trebesch, C., Schramm, S., Weiser, L., and Schade, C., "Ukraine Support Tracker Data," Kiel Institute for the World Economy, December 2025, https://www.kielinstitut.de/publications/ukraine-support-tracker-data-6453/

Early private-sector delivery reflects rapid mobilization in 2022. The peak observed in 2022-Q4 reflects the creation and leveraging of more structured coordination mechanisms and consolidated assistance packages as initial uncertainty gave way to clearer priorities.

Foreign government assistance follows a different pattern, with delayed but exponentially increasing committed and delivered CDA. The pronounced surge in 2025-Q1 corresponds to large, recorded tranches of aid linked to the establishment of coordination mechanisms such as the IT Coalition and Tallinn Mechanism.[7] The growing gap between commitments and deliveries of foreign government CDA across quarters reflects a key structural component of how governments operationalize CDA: governments have lengthy procurement and bureaucratic processes that extend implementation timelines.

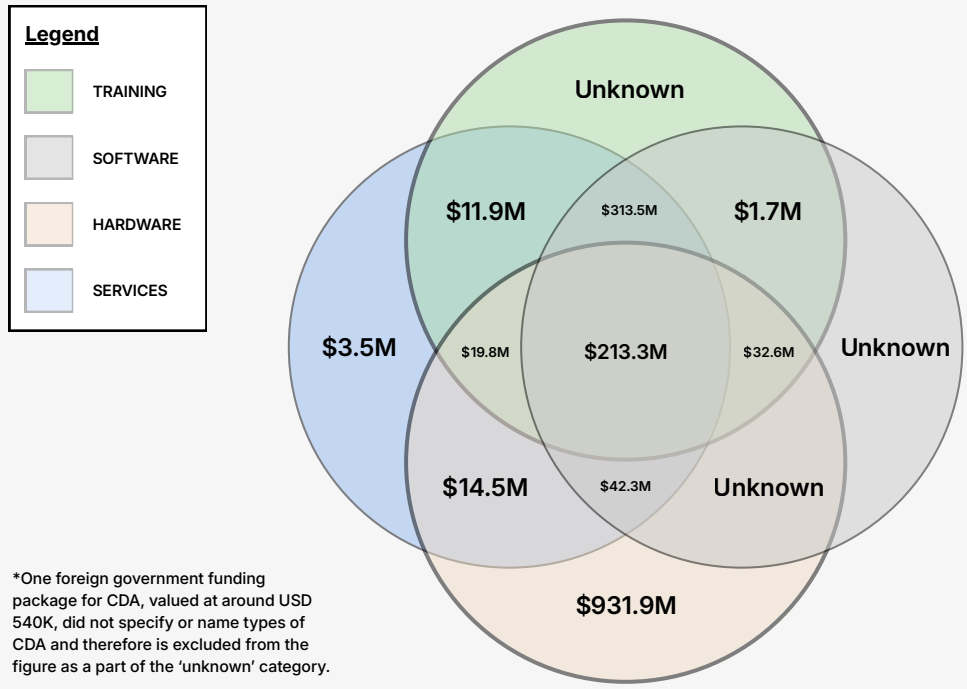
The next three sections of this report will further analyze CDA by provider type: foreign government, private sector, and coordination mechanisms.

7. See Appendix 1 for more information on the IT Coalition and Tallinn Mechanism.

Section 4. Foreign Governments

Foreign governments represent the largest source of disclosed CDA to Ukraine between 2022 and 2025, providing support through both bilateral aid and multilateral coordination mechanisms. Figure 4 below includes 49 confirmed foreign government CDA packages to Ukraine and attempts to depict the distribution of aid across the four types of CDA.[8] The data includes both delivered and committed aid totaling around USD 1.7B.[9]

Figure 4. Recorded Foreign Government CDA Type Breakdown



*One foreign government funding package for CDA, valued at around USD 540K, did not specify or name types of CDA and therefore is excluded from the figure as a part of the 'unknown' category.

Source: CDAC BFT Dataset released March 4, 2026

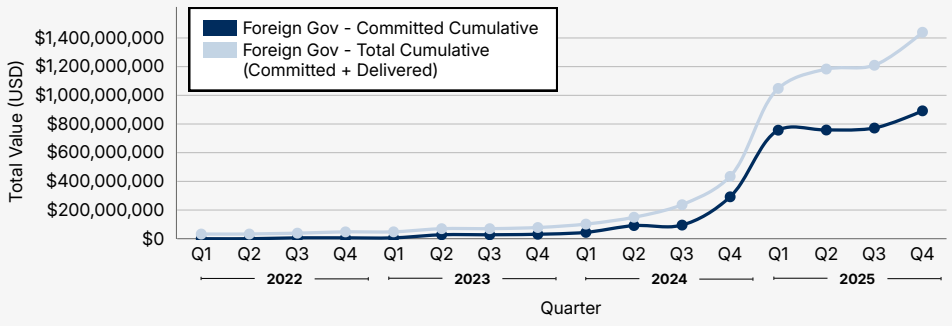
8. See Appendix 2 for more information on the types of CDA.
9. As mentioned in Section 2. Methodology & Limitations, a significant portion of this aid remains aggregated in packages. As a result, a substantial share of government-attributed funding cannot be precisely linked to a specific Ukrainian recipient or to CDA exclusively. These bulk and broader packages sum up to nearly USD 93.2M but are excluded from the report's figures and analysis.

Of the confirmed foreign government CDA delivered to Ukraine, nearly 80% of the packages include hardware. Standalone hardware procurement accounts for at least USD 930M, making hardware the single largest category of foreign government CDA value.

The data supports CDAC's insights regarding the critical need for hardware in Ukraine. The effectiveness of many software-driven interventions depends on a baseline level of infrastructure readiness, including compatible hardware. Where hardware is outdated or unsupported, the deployment of modern defensive tools becomes technically constrained. At the time of writing, several Ukrainian recipients are unable to implement advanced software solutions, such as endpoint detection and response (EDR) systems, because existing hardware infrastructure cannot support them, underscoring the critical importance of foundational equipment upgrades.[10]

Furthermore, examining the timeline of announced foreign government CDA highlights that significant increase in foreign government CDA–nearly USD 1.5B–correlated with the formalization of the IT Coalition and the Tallinn Mechanism. Figure 5 depicts this increase by showing foreign government CDA cumulating over each quarter.

Figure 5. Cumulative Foreign Government CDA by Quarter



Source: CDAC BFT Dataset released March 4, 2026

10. Roundtable at the Center for European Analysis (CEPA), Feb 2, 2026

Figure 5 also highlights that while foreign governments have committed around USD 883.5M, plans for delivery of funds or implementation of aid remain unclear. One anonymous international cyber policy expert noted that European aid packages typically take 24-60 months for delivery while US aid delivery could occur within 12 months.[11] Since a majority of the CDA to Ukraine committed by foreign governments through the IT Coalition and Tallinn Mechanism are sourced from European nations, the period between commitment and delivery lasts for many months.

Patterns in CDA between the European Union and the United States broadly align with wider aid and support trends identified by the Kiel Institute in early 2026.[12] European actors have increasingly assumed a leading role in CDA delivery, both in aggregate value and in continuity of support as US assistance took a sharp decline after January 2025.[13] Appendix 3 includes a further breakdown of foreign government aid by the United States, the European Union, and Estonia.

11. Marianna Fakhurdinova, "Wartime Assistance to Ukraine: The Successes, Failures, and Future Prospects of US and EU Support Models," CEPA, January 15, 2026, https://cepa.org/comprehensive-reports/wartime-assistance-to-ukraine-the-successes-failures-and-future-prospects-of-us-and-eu-support-models/.
12. Antezza et. al, "Ukraine Support Tracker Data," Kiel Institute for the World Economy.
13. Christoph Trebesch and Taro Nishikawa, "Kiel Policy Brief February 2026 Europe Steps up: Ukraine Support after Four Years of War," Kiel, February 2026, https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/dd24a73f-4270-46c5-9c40-bcc9df4f1672-KPB2023_EN.pdf.

Section 5. Private Sector

The private sector plays an indispensable role in the delivery and effectiveness of CDA, especially given that private firms remain the primary producers, operators, and protectors of the digital ecosystem.[14] Since 2022 companies have responded rapidly by donating large amounts of resources such as cybersecurity software, licenses, training credits, and expertise.[15] The private sector has delivered CDA through direct corporate contributions (i.e., in-kind support or discounted services) and through coordination mechanisms.

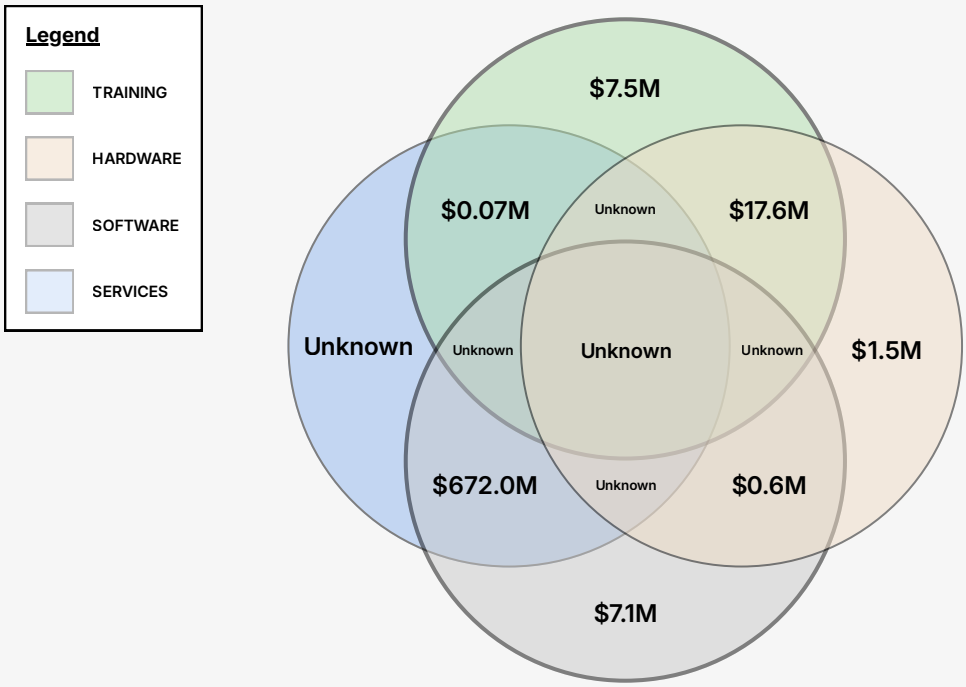
Additionally, while a majority of foreign government CDA to Ukraine delivered hardware, sustaining wartime cyber defense also depends on continuous operational support that keeps systems functional over time.[16] The private sector filled in these gaps of training and software deployment.

In publicly-disclosed values, private-sector CDA totals approximately USD 706.1M across 67 recorded aid mentions from 41 providers worldwide, predominantly based in Europe and the United States. Unlike government aid—which comes in large 'packages'—the private sector has delivered CDA through a large number of smaller and quicker deliveries or 'transactions'.

Figure 6 below breaks down the known private-sector CDA values by type of assistance and includes both publicly-disclosed information and recorded CDAC deliveries.

14. Greg Rattray and Seungmin Helen Lee, "Cyber Defense Assistance and Ukraine," Aspen Digital, April 1, 2025, https://www.aspendigital.org/report/cyber-defense-assistance-ukraine/.
15. Louise Axon et al., "Private-Public Initiatives for Cybersecurity: The Case of Ukraine," Journal of Cyber Policy 9, no. 3 (February 5, 2025): 399–422, https://doi.org/10.1080/23738871.2025.2451256.
16. Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," Carnegie Endowment for International Peace, November 3, 2022, https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense.

Figure 6. Recorded Private-Sector CDA Type Breakdown



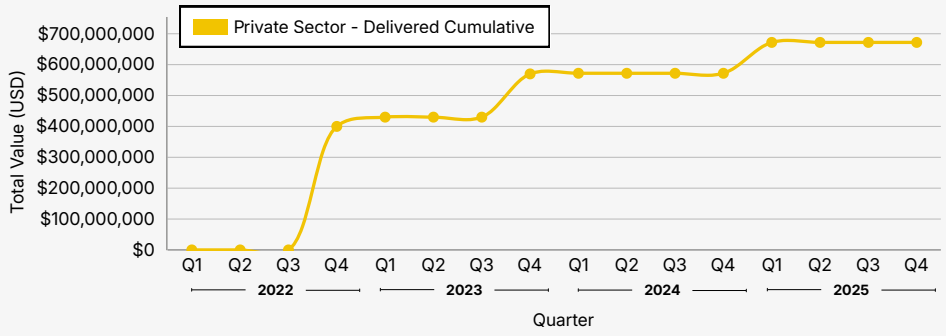
Source: CDAC BFT Dataset released March 4, 2026

Figure 6 shows that combined software and services constituted the dominant share, accounting for approximately 95% of private-sector CDA value across 94 transactions. Software is mentioned in 55 transactions. Training follows behind, constituting 2% of the value through 29 transactions. This analysis indicates that companies were able to provide training frequently at a relatively low cost per engagement.

On the other hand, hardware, whether standalone or combined with software, represented a small fraction of private-sector CDA: only 0.3% of known private-sector CDA values across 5 datapoints mentioned hardware. Overall, Figure 6 highlights that delivering software and training may be less costly and less challenging than physically delivering hardware to a nation at war.

An examination of the timeline for private-sector CDA reveals further differences between foreign government and private-sector CDA. Figure 7 below demonstrates the timeline of cumulative private sector CDA by quarter between 2022 and 2025.

Figure 7. Cumulative Private-Sector CDA by Quarter



Source: CDAC BFT Dataset released March 4, 2026

Private-sector CDA delivery underwent rapid mobilization and had a significant spike at the end of 2022, not even a full year after the full invasion of Ukraine. However, unlike the foreign government CDA, the cumulative private sector CDA has only increased by approximately USD 106M between Q4 of 2023 and Q4 of 2025. 84.3% of the private-sector CDA was delivered in the first year of the war, highlighting early motivation to support Ukraine as well as a drop in aid due to donor fatigue starting in 2024.[17]

Finally, while the status of foreign government CDA remains committed for many months at a time, undergoing lengthy procurement and budget cycles, private-sector CDA is committed and delivered in a much quicker turnaround. CDAC records indicate that CDA could be delivered within 48 hours of a request, especially when the request was for vouchers and certificates for training.

17. Yevheniia Yefymoya and Seungmin Helen Lee, "Donors' Voices in Assisting Ukraine's Cyber Defense: Drivers of Early Support & Barriers to Sustainment," Cyber Defense Assistance Collaborative (CDAC), November 26, 2025, https://crdfglobal-cdac.org/donors-voices-in-assisting-ukraines-cyber-defense-drivers-of-early-support-barriers-to-sustainment/.

Section 6. Coordination Mechanisms: Delivered & Open Requests

Many CDA packages involve multiple actors: governments, implementers, vendors, and Ukrainian recipients. Therefore, coordination mechanisms that organize delivery can increase speed and efficiency, assist with communication, improve situational awareness, and decrease duplicative efforts and requests. Within the Ukraine CDA ecosystem, coordination channels broadly fall into two functional models:[18]

1. **Multilateral, government-led coordination frameworks** designed to systematize donor support, such as the Tallinn Mechanism and the IT Coalition
2. **Civilian and private sector-led hubs** focused on operation and matching requests to capabilities, such as CDAC and Global Cyber Cooperative Center (GC3).[19]

As depicted in Figure 8 below, coordination mechanisms helped deliver at least 56.84% of the total recorded CDA value.

Figure 8. Channel-Based Allocation of Total CDA Value

Provider Type	Channel	Value (USD)	% of Total CDA
Private Sector	Unknown or N/A	675,000,000	29.45%
Private Sector	CDAC	31,534,603	1.38%
Foreign Government	Unknown or N/A	314,434,412	13.72%
Foreign Government	IT Coalition	946,437,585	41.29%
Foreign Government	Tallinn Mechanism	324,840,623	14.17%

18. See Appendix 1: Chart of Sample Donor Community
19. "ГЛОБАЛЬНИЙ ЦЕНТР ВЗАЄМОДІЇ В КІБЕРПРОСТОРІ (GC3)," GC3, accessed March 2, 2026, https://gc3.digital/.

For a coordination mechanism to function, the mechanism itself requires funding and resources to cover logistical and administrative costs, facilities, personnel to organize, and more. For example, the IT Coalition required at least USD 10.8M pledge from Luxembourg to launch the initiative.[20]

Once established, coordination mechanisms generally add value in two ways. First, they help generate or incentivize a prioritized list of requirements, which improves alignment and visibility across donors and reduces duplication.[21] Requested assistance also captures Ukrainian recipients' immediate and, over time, long-term needs. Currently, Ukrainian unmet needs across two coordination efforts total at least USD 128.7M, with USD 95.5M noted by Tallinn Mechanism and USD 32M by IT Coalition.[22] Immediate requests include American cybersecurity products as well as IT infrastructure, including the construction of secure data centers.[23]

CDAC also has open requirements for software and hardware. These requests have remained open for months to years due to a lack of funding and capability. One type of commonly recurring open requests include requests for extensions to software licenses: when in-kind donations of software licenses are delivered, they tend to be short-term licenses that sometimes only last a few months. The burden of requesting constant extensions over the four years of the war has increased friction in CDA delivery. Additionally, the prominence of open requests for training could potentially signal a broader shift towards longer-term cyber resilience and a self-sustaining model for cybersecurity.

20. "Luxembourg, Estonia and Ukraine Have Launched the IT Coalition," Ministerium für Gesundheit und soziale Sicherheit - Die Luxemburger Regierung, September 19, 2023, https://m3s.gouvernement.lu/de/agenda.gouvernement2024%2Bde%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2023%2B09-septembre%2B19-bausch-itcoalition.html.
21. Rattray and Lee, "Cyber Defense Assistance and Ukraine."
22. Roundtable at the Center for European Analysis (CEPA)
23. Roundtable at the Center for European Analysis (CEPA)

Second, these mechanisms can improve scalability and execution with a structured governance process. For example, the IT Coalition uses a recurring process to approve procurement packages, administers contributions through Luxembourg, and implements packages via the NATO Support and Procurement Agency (NSPA).[24]

Despite their advantages, coordination mechanisms face persistent structural challenges. By the end of 2025, visibility remained uneven, and coordination efforts remained largely operationally siloed. For example, establishing transparency between CDAC and the IT Coalition or the Tallinn Mechanism has been challenging.

Gaps in available data reflect inconsistent disclosure practices among providers and limited cooperation between coordination channels. As reporting and participation are frequently voluntary, significant portions of CDA remain unrecorded, creating challenges for assessing real CDA demand and identifying capability gaps. Consequently, no single actor possesses comprehensive visibility into the scale, composition, or timing of CDA delivered to Ukraine.

Coordination has also introduced administrative friction. Multilateral frameworks often operate within complex governance structures that slow decision making and aid delivery. This delay has been previously highlighted in this report. The delay in CDA delivery can reduce the efficacy of cyber defense during periods of rapidly evolving cyber threat activity.

24. "How the IT Coalition Enhances and Scales the Digital Capabilities of the Defence Forces of Ukraine," Ministry of Defense of Ukraine, March 20, 2025, https://mod.gov.ua/en/news/equipment-licenses-and-digital-services-how-the-it-coalition-enhances-and-scales-the-digital-capabilities-of-the-defence-forces-of-ukraine.

Section 7. Conclusion

CDA for Ukraine has evolved since 2022 into a layered and interdependent ecosystem. Over time, ad-hoc assistance evolved toward more structured, multilateral coordination, yet increased coordination has not fully resolved underlying visibility challenges: large portions of assistance remain categorized as unknown, reflecting fragmented reporting practices that complicate strategic planning and long-term projection of needs. Analyzing the available data, this report finds three emerging themes.

First, foreign government CDA takes the form of high-value funding packages, often remains in the 'committed' status for more than a year, and has been mostly directed towards hardware delivery. On the other hand, private-sector CDA takes the form of more often but smaller deliveries, can be delivered in days or months, and has mostly been software and training.

Second, coordination mechanisms can lead to the creation of a prioritized requirements list, leading to increased visibility and decreased duplication. Coordination mechanisms also could allow for improved scalability, execution, and repeatability with a structured governance process; however, despite the benefits, the mechanisms have also demonstrated proneness to administrative friction and inconsistent disclosure practices among providers.

Finally, analysis of requested CDA reveals that hardware continues to be a high-priority need but also that a movement towards requesting more training for longer-term resilience and domestic capabilities could be observed.

As the War in Ukraine enters its fifth year, the layered and interdependent CDA ecosystem will need to continue evolving to overcome challenges, increase efficiency, and support Ukrainian cyber defense needs.

Section 8. Appendix

Appendix 1: Chart of Sample Donor Community

Foreign Government	
United States	The single largest bilateral CDA provider (USD 202M+ disclosed by January 2026), combining monetary, services, and intelligence, and partnerships. Aid delivery, however, became uncertain in 2025 following a freeze on foreign aid and pauses in cyber operations.[25]
European Union	The European Union functions as a central donor emphasizing long-term civilian cyber resilience and institutional capacity building. Major contributors include Estonia, Denmark, Germany, France, and the Netherlands, operating through EU instruments, bilateral initiatives, and broader aid-coordination mechanisms.
Private Sector	
Google (Mandiant)	Provided platform security, threat intelligence, and incident response; notable for early, sustained engagement and for integrating cyber defense with counter-disinformation and cloud resilience.[26]
AWS	Enabled large-scale data migration and service continuity as the Russians targeted physical infrastructure with cyberattacks; its contribution supported cross-sector resilience.[27]
Microsoft	Microsoft and the Microsoft Threat Intelligence Center have played a critical role in the detection and response to cyber threats, as well as in Ukrainian data migration.[28]
Government-Led Coordination Efforts	
Tallinn Mechanism	Established in December 2023, the Tallinn Mechanism is a government-led multilateral framework designed to coordinate civilian cyber assistance to Ukraine. Founding participants include Estonia, Canada, Denmark, France, Germany, the Netherlands, Poland, Sweden, Ukraine, the United Kingdom, and the United States. The mechanism focuses primarily on identifying needs, matching donors to priorities, and supporting long-term civilian cyber resilience.[29]
IT Coalition	Established in September 2023 under the Ukraine Defense Contact Group ("Ramstein") framework, the IT Coalition is a multilateral initiative focused on supporting Ukraine's Ministry of Defense and Armed Forces' military IT, communications, and cybersecurity capabilities. The coalition includes 17 participating nations, led by Estonia and Luxembourg, and operates through pooled funding as well as direct in-kind contributions. Financial contributions are administered by Luxembourg and implemented through the NATO Support and Procurement Agency.[30]
Civilian-Led Coordination Efforts	
GC3	Global Cyber Cooperative Center (GC3) is a Ukrainian-based think-tank and cyber-security trust hub established in 2019. Its mission is to develop productive cooperation between public and private creators of safe cyberspace and strengthen national cybersecurity through strategic global partnerships.[31]
CDAC	The Cyber Defense Assistance Collaborative (CDAC) is a non-profit initiative that coordinates CDA by aligning private-sector technology and cybersecurity companies with Ukrainian recipients including Naftogaz, UkrTelecom, and the Ukrainian government. CDAC serves as a bridge to private sector capabilities and cyber expertise to support Ukraine's cyber defense.[32]

25. Siim Alatalu, "Is America Surrendering Its First Line of Cyber Defence?," International Centre for Defence and Security, March 10, 2025, https://icds.ee/en/is-america-surrendering-its-first-line-of-cyber-defence/.
26. Lauren Bassett, "Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare," Cambridge Journal of Political Affairs, 2024, https://www.cambridgepoliticalaffairs.co.uk/2025/01/14/silicon-shadow/#section3.
27. Bassett, "Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare."
28. Bassett, "Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare."
29. Rattray and Lee, "Cyber Defense Assistance and Ukraine."
30. "How the IT Coalition Enhances and Scales the Digital Capabilities of the Defence Forces of Ukraine."
31. "ГЛОБАЛЬНИЙ ЦЕНТР ВЗАЄМОДІЇ В КІБЕРПРОСТОРІ (GC3)."
32. "Cyber Defense Assistance Collaborative (CDAC)"

Appendix 2: Types of Cyber Defense Assistance

This analysis categorizes the cyber defense assistance provided to Ukraine into four core components: Training, Services, Hardware, and Software.

CDA Type	Definition	Example
Hardware	Hardware devices can perform core network and device protection and include: physical components of IT and OT systems, routers, switches, firewalls, IDS/IPS appliances, industrial controllers, IoT/OT sensors and consoles.	In May 2024, Latvia delivered around USD 108K worth of communication equipment to Ukraine's Ministry of Defense through the IT Coalition.[33]
Software	Software includes security applications, analytics and control programs, platforms, and tools that run on hardware to detect, analyze, or mitigate threats.	In January 2023, SAP provided 1,000 software licenses free of charge to Ukrainian military users, giving them direct access to enterprise software tools to support operational and logistical functions.[34]
Services	Services include outsourced support and managed offering such as consulting, incident response, testing, and intelligence sharing.	In March 2022, Google Cloud expanded Project Shield to provide free, unlimited DDoS protection to Ukrainian public-sector and humanitarian entities, backed by its Cybersecurity Action Team.[35]
Training	Training includes courses and certifications that build cybersecurity skills and capacity.	In December 2025, experts from Japan's Ministry of Defense and the Japan Self-Defense Forces ran a workshop on the implementation of NIST-based Risk Management Framework with Ukraine's Ministry of Defense and Armed Forces.[36]

33. "It Коаліція: Латвія Передала Україні Обладнання: Новини МОУ," IT коаліція: Латвія передала Україні обладнання | Новини МОУ, May 7, 2024, https://mod.gov.ua/news/it-koalicziya-latviya-peredala.
34. SAP News, "Reaffirming SAP's Support for Ukraine," SAP News Center, January 20, 2023, https://news.sap.com/2023/01/reaffirming-support-for-ukraine/.
35. Phil Venables, "Google Cloud's Security and Resiliency Measures for Customers and Partners," Google Cloud Blog, March 3, 2022, https://web.archive.org/web/20221227055541/https:/cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine.
36. "Japan's Ministry of Defense Shares Cybersecurity Expertise with Ukraine under the IT Coalition," Ministry of Defense of Ukraine, December 9, 2025, https://mod.gov.ua/en/news/japan-s-ministry-of-defense-shares-cybersecurity-expertise-with-ukraine-under-the-it-coalition.

Appendix 3: Foreign Government CDA – the US, the EU & Estonia

The United States (US)

United States — Total (Delivered + Committed)	USD 202,000,000
United States — Delivered	USD 82,000,000
United States — Committed	USD 120,000,000

The United States used to be the single largest contributor of recorded civilian cyber assistance to Ukraine, with a total of USD 202M in delivered and committed funding. US support was delivered primarily through bilateral channels and federal agencies, most notably USAID.

The largest single program is the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, valued at USD 120M. This program sought to strengthen the resilience of Ukraine's critical infrastructure against cyberattacks and was initiated in April 2019, before the Russian full-scale invasion. While the program concluded in April 2023, the activity had reflected a longer-term US engagement in Ukrainian cyber resilience.[37]

Notably, observed US cyber aid contracted sharply in 2025. Only USD 14M was recorded and contributed as part of a larger Tallinn Mechanism package. This reduction reflects the broader contraction of US foreign assistance following the January 2025 administrative transition and the dismantling of USAID, which had served as the primary delivery vehicle for US cyber assistance to Ukraine.

37. Robert P Storch, Cardell K Richardson, and Paul K Martin, "Operation Atlantic Resolve Including U.S. Government Activities Related to Ukraine," Special Inspector General Report to the United States Congress, 2024, https://oig.usaid.gov/sites/default/files/2024-11/OAR_Q4_Final.pdf.

The European Union (EU)

EU — Total (Delivered + Committed)	USD 217,317,061
EU — Delivered	USD 97,102,128
EU — Committed	USD 120,214,933

The European Union has been a major supporter of Ukrainian cyber defense, delivering aid through bilateral support or aid channels such as the IT Coalition and the Tallinn Mechanism. EU approaches play an increasingly dominant role, with primary leadership of CDA to Ukraine led by Estonia and Luxembourg. Key initiatives involve deploying cyber rapid-response teams, providing access to an EU Cybersecurity Reserve, and establishing cyber labs for military training.

Estonia

Estonia — Total (Delivered + Committed)	USD 37,846,038
Estonia — Delivered	USD 1,128,668
Estonia — Committed	USD 38,974,706

Estonia receives particular attention in this report, given its leadership role in civilian digital assistance to Ukraine: it is a founding member of the Tallinn Mechanism through the Estonian Centre for International Development (ESTDEV) and a co-lead nation of the IT Coalition alongside Luxembourg.[38] Estonia's CDA has flowed primarily through these two multilateral mechanisms.

38. Matthew Crandall, "Understanding Estonia's Cyber Support for Ukraine: Building Resilience, Not Status," Applied Cybersecurity & Internet Governance, July 5, 2024, https://doi.org/10.60097/acig/190396.

Through the IT Coalition, Estonia reportedly contributed USD 2.7M in 2024 and USD 10.1M in 2025, of which USD 3.95M went towards the purchase of Starlink communication systems. For 2026, Estonia is planning on over USD 5.9M in contributions to the IT Coalition. The nation's contributions to the Tallinn Mechanism include USD 1.02M in 2024–2025 and a pledge of USD 580K for 2026.[39]

Publicly, Estonia committed USD 28.4M through the Tallinn Mechanism at the end of 2025. The funding will go through an international procurement framework and be delivered between 2025 and 2030.[40] In a broader context, Estonia's total military and non-military assistance to Ukraine since 2022 exceeds USD 1.18B, of which approximately one-third is civilian and the remainder military.

39. The figures draw on information verified with Estonian officials. However, it is unclear if and how these figures overlap with publicly known Estonian CDA and thus the BFT dataset does not include this information.
40. "Estdev and Partners Announce an International Procurement for the Implementation of Cybersecurity Projects until 2030," ESTDEV, November 13, 2025, https://estdev.ee/en/articles/estdev-and-partners-announce-international-procurement-implementation-cybersecurity.


CDAC
A CRDF GLOBAL INITIATIVE