ASPEN DIGITAL
aspen institute

THE CYBER DEFENSE ASSISTANCE IMPERATIVE
LESSONS FROM UKRAINE

FEBRUARY 2023

Authors

Greg Rattray, Founder, Cyber Defense Assistance Collaborative (CDAC); Founder, NextPeak; Former CISO, JPMorgan Chase

Geoff Brown, Participant, CDAC; Vice President, Recorded Future; Former CISO, NYC & Head of NYC Cyber Command

Robert Taj Moore, Director, Aspen Cybersecurity Group, Aspen Digital

Contributors

Michael Daniel, President & CEO, Cyber Threat Alliance

Jeff Greene, Senior Director of Cybersecurity Programs, Aspen Digital

Stacy O'Mara, Senior Leader of Global Government Strategy, Affairs, and Partnerships, Mandiant

I. Introduction

Russia's further invasion of Ukraine in February 2022 was a watershed moment. Governments, citizens, and companies faced a choice—they could support Ukraine in its fight to defend its independence or they could sit back while Russia destroyed the post-war order that has stood since 1945. On an unprecedented scale, a major nation-state had engaged in coordinated, convergent digital and physical attacks in an effort to conquer a neighboring country. Ukraine's response to Russian aggression was multi-faceted, and leveraged a wide range of assistance from many sources.

Historians, strategists, and politicians will draw lessons from this conflict for years, but one is already clear: effective, adaptable cyber defense will be essential in future conflicts, and thus the ability to deliver cyber defense assistance must be a key national security capability. Examining how partners delivered cyber defense assistance to Ukraine can teach us how to conduct similar operations successfully in the future.

Many Western companies chose to help Ukraine defend its government and critical infrastructure in cyberspace. These efforts have enhanced Ukraine's resiliency. However, they were largely organized on the fly, either in the immediate run-up to the conflict or in the midst of the war. Unfortunately, the current state of geopolitics, as well as the reality that many nation-states do not have adequate operational cyber defense capabilities, suggests this will not be the last time the private sector and Western governments need to provide cyber assistance to a besieged nation.

Informed by the ongoing work of a variety of organizations providing operational cyber support to Ukrainian institutions through the Cyber Defense Assistance Collaborative, this paper seeks to define cyber defense assistance, outline its primary component parts, and identify key lessons learned that can help inform how such assistance can be provided in future geopolitical conflicts. It makes the case that an effective national security toolkit requires the ability to deliver cyber defense assistance to allies.

II. What is Cyber Defense Assistance and its Benefits?

For the purpose of this paper, "cyber defense assistance," or CDA, refers to cyber support activities provided to friendly or allied nation-states under threat of or actual attack from a hostile nation-state. Unlike traditional cyber capacity building, CDA is geared toward achieving specific national security objectives. While general capacity building does not always center on a specific threat, CDA is responsive to discrete geopolitical risks. Cyber defense assistance is unique in another important way—unlike other national security efforts, such as counterterrorism and nonproliferation, the private sector is indispensable to its delivery and success.

To date, cyber defense assistance has been aimed at meeting more immediate needs—primarily providing operational cyber support to Ukraine in the run-up to and early stages of Russia's February 2022 invasion. However, CDA activity will not always be exigent, and can take the form of pre- or post-conflict capability enhancements. Nonetheless conflict-driven national security objectives should always guide CDA decision-making.

> **Cyber defense assistance can be defined as cyber support activities provided to friendly or allied nation-states under threat of or actual attack from a hostile nation-state.**

Cyber defense activities can include:

- Vulnerability Management (VM) intelligence and technologies
- Security Information and Event Management (SIEM) systems and data analysis assistance
- Distributed Denial of Service (DDOS) mitigation technologies and service offerings
- Access to intelligence platforms (for cyber threat intelligence and associated analysis requirements), and professional cyber intelligence analyst access
- Attack Surface Monitoring (ASM) and intelligence, as well as threat surface enumeration assistance
- Executive engagement for information on cyber organizational structures, programs, policies, and processes
- Malware and technical attack forensics
- Compromise Assessment and Incident Response (CAIR) services
- Endpoint Detection and Response (EDR) and anti-virus technology offerings
- Security Operations Centers (SOCs) design
- Industrial Control System (ICS) associated cybersecurity expertise and offerings

While these are part of a core set of CDA activities, the nature of the assistance must continually evolve as adversaries and the threats they pose change. CDA must also be tailored to a recipient's existing capabilities. Governments and key private sector partners must have a capacity to deploy such assistance rapidly in a wide range of situations.

CDA activities can serve several purposes. In the months preceding a potential conflict, they can help deter aggression by strengthening a recipient nation's resilience and reducing an aggressor's confidence in its offensive capabilities. During a conflict, CDA efforts can help mitigate the impacts of cyberattacks by buttressing the capabilities and will of recipients to prevail. Post-conflict, CDA programs can help the recipient nation return to normal and remove lingering aggressor presence in its networks, as well as to provide a bridge to more traditional, longer-term capacity building initiatives (*e.g.,* developing a body of statutes to address cybercrime, training prosecutors, conducting hackathons, etc.). Additionally, CDA could help achieve post-conflict stability goals by making recipients more capable of withstanding future cyber aggression.

Both public and private entities might conduct or support such CDA activities, including government organizations, cybersecurity companies, technology platform providers, as well as non-profits conducting cyber and technology assistance. However, regardless of who sponsors the support, effective CDA efforts will rely on private sector expertise and capabilities because private companies are the primary entities capable of providing adaptable and scalable tools and services quickly and across the globe. The right mix of companies organized effectively can help potential assistance recipients understand the range of available capabilities and can also facilitate the successful matching of tools and services with a potential recipient, all based on the recipient's specific technology base and skills. A complex web of government organizations, private companies, as well as non-profit organizations will likely carry out and support these activities, as is the case in many conflict situations. Tracking and synchronizing such activities will add to their impact.

In the case of the Ukraine conflict, the Cyber Defense Assistance Collaborative (CDAC), a volunteer group drawn from Western cybersecurity companies and organizations, provided a significant level of cyber defense assistance. The CDAC organizations' efforts to provide coordinated threat intelligence, technology capabilities, support services, and advice to assist Ukraine's government and critical infrastructure entities offer valuable lessons going forward.

III. The Cyber Defense Assistance Collaborative for Ukraine [1]

CDAC is a volunteer group of cybersecurity and technology organizations that sought to provide intelligence, technology, training, advisory, and other services to Ukrainian institutions. Its original goal in Ukraine was to enhance Ukrainian cyber defenses and protect Ukrainian critical infrastructure under the exigent circumstance of Russia's February 2022 invasion. CDAC's goal has since expanded to include improving the stability and ongoing protection of Ukrainian organizations by reducing or mitigating potential effects of cyberattacks. CDAC has also assisted select Ukrainian organizations in building resilient and secure digital systems in anticipation of future Russian campaigns to degrade Ukraine's physical, digital, and societal integrity.

---

[1] CDAC is just one example of this kind of support, as other organizations delivered significant cyber, tech, and telecommunications resiliency assistance–and continue to do so at the time of this report. This includes actions to enable satellite communications as well as work to help Ukrainian organizations move data and tech operations to cloud environments.

> “Necessity is the mother of all invention.”
> A proverb, attributed to Plato

CDAC efforts began informally, immediately after the February invasion. The initial volunteers leveraged existing connections with the leadership of Ukraine’s National Cybersecurity Coordination Center (NCCC) to understand how private sector cybersecurity companies could provide assistance of immediate benefit. The same group then engaged leadership of key technology and cyber companies to explore what tools and services they could provide voluntarily, outside of traditional software, hardware, or services sales channels.

CDAC participants recognized that a country at war may require help identifying and facilitating the production of cyber defense assistance, and provided that support. The interested private sector parties then agreed to coordinate their individual efforts under the moniker of the “Cyber Defense Assistance Collaborative for Ukraine,” which provided a forum to receive requests for assistance and to coordinate the delivery of support. In the case of Ukraine, wartime exigencies necessitated direct contact between Ukrainian operators and assistance-providing organizations in order to figure out what the most useful assistance might be. Those contacts grew quickly, as more Ukrainian organizations expressed a need for improved threat intelligence capabilities, licenses, and training for cyber defense tools.

CDAC operations help provide high impact results through the orchestrated actions of its participants. First, CDAC for Ukraine is a voluntary group operating with a high degree of openness; it seeks to share lessons learned and provide support that combines the information and knowledge of its participants. Second, the Ukrainian organizations seeking assistance have a long-term partner focused on enhancing the overall cyber defense of the nation.

4 Primary Categories of CDAC Assistance

1. Intelligence analysis, support, and sharing

CDAC participants share reports, artifacts, and access to commercially available intelligence platforms. This intelligence is derived from sources accessible through open-source research, or through the commercial purchase of data sets, and undergoes significant technical processing proprietary to the individual companies involved. It is also available for machine analysis and integration, or for human use. This intelligence is intended to facilitate the detection and mitigation of Russian cyber activities, as well as to support the investigative work needed to identify and expose Russian cyber influence activity.

2. Licenses

CDAC participants provide licenses for cyber defense technologies and associated services to address immediate, tactical needs to protect against and detect cyber threats. Technologies have included EDR tools, vulnerability scanners, forensic tools, security orchestration and response (SOAR) technologies, threat intelligence platforms (TIPs), cloud security products, or network and application security technologies (like virtual firewalls or malicious network traffic mitigation capabilities).

3. Tactical Services

CDAC participants have also provided to Ukrainian organizations various kinds of tactical services. Examples include refining specific requests for assistance, communicating priorities via Ukrainian hub partners, and helping to sustain connections through completion of delivery.

CDAC for Ukraine has extended these tactical efforts to assisting key governmental and critical infrastructure operators with security operations uplift. These efforts have begun to focus on helping Ukrainian operators understand enterprise-level cyber defense requirements; architect the tools, data, and analytics necessary to monitor and alert on attacks; and provision tools and assist in ensuring proper configuration and analytic training. There are also other efforts and service support, such as SOC-development assistance for large government and critical infrastructure companies, which is an extended, multi-month activity with deep investment in time and effort by those participating in the assistance. Additional support has included incident response services to public and private sector entities throughout Ukraine.

4. Advising

CDAC participants have become trusted advisors and partners to Ukrainian organizations in their ongoing establishment of national cyber defense approaches. CDAC participants understand and are conversant in the capabilities needed to build and operate enterprise cybersecurity programs. For example, at the time of this report, CDAC participants are assisting in senior leader education for government and critical infrastructure organizations. CDAC participants also plan to assist the Ukrainians with the establishment of organizations to exercise and assess a wide range of Ukrainian cyber defense capabilities.

In the provision of these intelligence, technical, and other advisory and support services, CDAC group participants remain individually responsible for their own corporations' adherence to technology transfer regulatory and compliance concerns. CDAC is non-binding and voluntary. Participating companies have mature cybersecurity offerings, and most are recognized leaders in the industry with significant experience in international intelligence, security technology deployment and operations, and civilian and military international government relations. Activities are discussed, collaborated on, and deconflicted in an entirely voluntary capacity by the group (holding multiple weekly discussions between employees of the participating companies), and conducted in direct coordination with Ukrainian government and critical infrastructure representatives. As cyber defense efforts for Ukraine involve multiple stakeholders across government, the private sector, and non-profit organizations, CDAC's orchestration of defense support activities can encourage deconfliction and increase transparency between organizations and sectors.

IV. Establishing Cyber Defense Assistance – Lessons from Ukraine

The effort in support of Ukraine has shown that effective CDA faces substantial challenges. Over the course of operations since late February 2022, the CDAC has endeavored to learn lessons and evolve. The lessons from Ukraine can be used to establish efforts in other contexts and areas of the globe. Key lessons include:

Need to Establish Early Connections and Trust Between Assistance Recipients and Capability Providers.

Connecting providers and recipients is not easy. Establishing the necessary relationships, enacting a process to collect assistance requests, and matching those requests to capability providers takes time, patience, and broad knowledge of both potential providers and recipients. CDAC for Ukraine's success bridging requests and capability providers was a result, in part, of the pre-existing relationships that participants had to Ukraine's national security leadership. For example, prior to the expanded invasion, CDAC's creators were involved for several years with helping Ukraine establish its national cyber strategy and response program. This long-term relationship was critical to creating the trust that allowed for the rapid communication of specific assistance requests from Ukrainian organizations to those companies that could provide cyber defense assistance. As another example, the ability of Ukrainian hub organizations to communicate requirements to CDAC, and to connect CDAC capability providers to key personnel in recipient organizations, was in part a result of the early connections and relationships that had been developed prior to the expanded invasion.

As with all types of operational collaboration, people and teams working together to improve specific capabilities—such as understanding the current weaknesses in an enterprise defense posture, volunteering cyber threat intelligence and analysis, improving ability to detect attacks, and training operators on the more effective use of tools—provides the essential foundation of cyber defense assistance. But this will not always be the case. As a result, as CDAC and other assistance providers consider providing cyber defense assistance in other contexts, they must prioritize the development of personal relationships between key players; initiating proactive cyber projects between assistance providers and recipients can greatly improve chances for success. Importantly, and as with other types of assistance, understanding the culture, language, and management approaches of the recipients has proven crucial to success

Need to Identify, Assemble, and Organize Capability Providers.

CDA will not work without a critical mass of capability providers. In the case of Ukraine, finding potential cyber defense assistance providers for Ukraine proved relatively easy. Russia's unprovoked aggression and brutal approach to the conflict violated clearly established norms that created a compelling moral justification companies could rely on to justify support for Ukraine. Additionally, in some cases, companies did not have a significant presence in or business ties to Russia, which made decoupling from the region relatively straightforward. However, the circumstances of other conflicts may create different conditions and make it more difficult to assemble a coalition of capability providers. As a result, it is critical to identify, assemble, and organize capability providers as early as possible so they can plan the kind of support they might need to provide and to whom.

Once assembled, organizing the providers and identifying what they can do is critical, and requires understanding how to package the diverse potential capabilities in a manner that could be readily communicated to potential recipients. Assistance recipients need to know exactly what they can and cannot expect in terms of support, so clearly communicating the capabilities of potential providers is essential. Without clarity, the creation and implementation of efforts will be less efficient.

An important CDAC attribute that helped increase participants' willingness to engage was the commitment that the coalition would

---

[2] In the case of potential U.S.-government-provided CDA to a recipient nation, government needs to do more to understand the scope of the legal authority of key government institutions to collaborate with private sector assistance providers.

provide only defensive assistance. This set expectations at the outset and allowed Ukraine to find other sources for offensive assistance. Additionally, as Ukrainian organizations have asked CDAC to engage in assistance projects that are broader in scope, the diverse capabilities of CDAC's participants have proven to be valuable. CDAC assistance projects that leverage multiple providers in a coordinated manner can deliver more strategic uplifts in capabilities (such as in unified security operations) that stand to have strategic benefits in national cyber resiliency and conflict stability going forward. Over time, sustaining and scaling the effort has been limited by CDAC's capacity to coordinate requests and mobilize participants (either individually or as a team). The Ukrainians need and are asking for more than CDAC can effectively organize. CDAC leadership is working to make CDAC's participants and recipients more efficient in orchestrating their overall capacity and delivery as well as grow the core project management capability of the CDAC and its Ukrainian hub partners.

Need to Align Activities and Establish Priorities.

Numerous Ukrainian organizations sought and continue to seek sources for cyber assistance. Similarly, many Western governments, companies, and even individuals are providing assistance in a variety of forms with differing arrangements, both paid and unpaid. These efforts are, for the most part, not coordinated with or transparent to each other. While there do not appear to be specific detrimental impacts from uncoordinated efforts, the assistance has largely been guided by ad hoc activities to support the near term needs and abilities of specific organizations or technologists that found a channel for getting help. The initiation of this range of activities occurred naturally as Ukrainians and those who wanted to help found each other. However, several months into the conflict, it

has been difficult to scale this initiative. CDAC's and others' efforts to provide assistance are not yet mature enough to build assured cyber defense capabilities that Ukrainians can operate in order to sustain successes as the conflict progresses and as post-conflict opportunities for reconstruction and stability arise.

Additionally, in the intelligence space, CDAC participants often observed a lack of well-defined requirements that are necessary to help the intelligence providers shape and curate collection, as well as to conduct analysis tailored to specific recipients. Currently, the Ukrainian organizations involved may only be ready to consume intelligence and react in an ad hoc fashion, but with appropriate preparation a recipient of cyber defense assistance will be able to more readily operationalize the intelligence and improve their cyber defense posture.

In short, CDAC and others providing assistance could achieve more through greater investment in hubs to coordinate activity, full-time management of assistance projects, and deeper contact between leaders and operators on both sides. Increasing the level of collaboration by like-minded governments would also enhance the efficacy of the assistance by ensuring the mutual awareness of "blue force" activities and helping resource sustained efforts achieve maximum benefits. As of this writing, CDAC has only been able to conduct limited convenings of a partial set of the organizations involved and participants are unaware of any other ongoing "blue force" tracking activities.

Further, CDAC has not yet developed the ability to collect, combine, and assess information on the cyber conflict in Ukraine. CDAC could create a foundation for doing so by borrowing from an Institute of War initiative that fuses public information in order to make transparent, trusted assessments of the conflict in the Ukraine. CDAC could do the same, and

with a focus on the cyber dynamics of the conflict in Ukraine and the factors that determine the success of cyber defense efforts. With a better understanding of the overall scale and impact of cyber defense assistance efforts, CDAC and other entities providing assistance will be better equipped to establish and invest in cyber defense assistance programs and capabilities.

V. Conclusion

Cyber defense assistance in Ukraine is working. The Ukrainian government and Ukrainian critical infrastructure organizations have better defended themselves and achieved higher levels of resiliency due to the efforts of CDAC and many others. But this is not the end of the road—the ability to provide cyber defense assistance will be important in the future. As a result, it is timely to assess how to provide organized, effective cyber defense assistance to safeguard the post-war order from potential aggressors.

The conflict in Ukraine is resetting the table across the globe for geopolitics and international security. The US and its allies have an imperative to strengthen the capabilities necessary to deter and respond to aggression that is ever more present in cyberspace. Lessons learned from the ad hoc conduct of cyber defense assistance in Ukraine can be institutionalized and scaled to provide new approaches and tools for preventing and managing cyber conflicts going forward.

Aspen US Cybersecurity Group

The Aspen US Cybersecurity Group is the nation's leading cross-sector, public-private cybersecurity forum comprising former government officials, Capitol Hill leaders, industry executives, security practitioners, and respected voices from civil society. It aims to translate pressing cybersecurity conversations into action.

Members

Congresswoman Yvette Clarke, Co-Chair, U.S House of Representatives

Christopher Krebs, Co-Chair, Senior Newmark Fellow in Cybersecurity, Aspen Digital

Katherine Adams, Senior Vice President and General Counsel, Apple

General (Ret.) Keith Alexander, President and CEO, IronNet Cybersecurity

Marene Allison, Vice President and CISO, Johnson & Johnson

Sara Andrews, CISO, Experian

Monika Bickert, Head of Product Policy and Counterterrorism, Facebook

Geoff Brown, Vice President, Recorded Future

Tom Burt, Corporate Vice President, Customer Security and Trust, Microsoft

Vinton G. Cerf, Chief Internet Evangelist, Google

Dr. Lorrie Cranor, Director, CyLab Security & Privacy Institute

Michael Daniel, President, Cyber Threat Alliance

Noopur Davis, Corporate EVP, Chief Information Security and Product Privacy Officer, Comcast

Jim Dempsey, Executive Director, Berkeley Center for Law & Technology

Donald R. Dixon, Co-Founder & Managing Director, ForgePoint Capital

Lucy Fato, Executive Vice President & General Counsel, AIG

Sue Gordon, Rubenstein Fellow, Duke University

Yasmin Green, CEO, Jigsaw, Google

Vishaal Hariprasad, Co-founder and CEO, Resilience

Niloofar Razi Howe, Senior Operating Partner, Energy Impact Partners

Aspen US Cybersecurity Group

Members (continued)

Congressman Will Hurd, Managing Director, Allen & Company LLC

Sandra Joyce, Executive Vice President, Mandiant Intelligence

Sean M. Joyce, Head of Global and US Cybersecurity and Privacy, PwC

Jodie Kautt, Vice President, Cyber Security, Target

Sam King, CEO, Veracode

Dr. Herb Lin, Senior Research Scholar for Cyber Policy and Security, Stanford University

Brad Maiorino, Corporate Vice President and CISO, Raytheon Technologies

Jeanette Manfra, Global Director for Security and Compliance, Google

Chandra McMahon, CISO, CVS Health

Dr. David McQueeney, Vice President, Corporate Technology & Community, IBM Corporation

Tim Murphy, Chief Administrative Officer, Mastercard

Craig Newmark, Founder, Craig Newmark Philanthropies

Dr. Gregory Rattray, Adjunct Professor, Columbia University SIPA

Nasrin Rezai, Senior Vice President and CISO, Verizon

David Sanger, National Security Correspondent, The New York Times

Dr. Phyllis Schneck, Vice President and CISO, Northrop Grumman Corporation

Bruce Schneier, Fellow, Berkman-Klein Center & Lecturer, Harvard Kennedy School

Alex Stamos, Adjunct Professor, Stanford University

Bobbie Stempfley, Vice President and Business Unit Security Officer, Dell Technologies

Scott C. Taylor, Strategic Advisor and Former General Counsel

Dr. Hugh Thompson, Managing Partner, Crosspoint Capital Partners

Jack Weinstein, Professor**,** Boston University

Dr. Jonathan W. Welburn, Researcher, RAND Corporation

Michelle Zatlyn, Co-founder & COO, Cloudflare

Jonathan Zittrain, Professor of Law and Professor of Computer Science, Harvard University


AD
ASPEN
DIGITAL
aspen institute