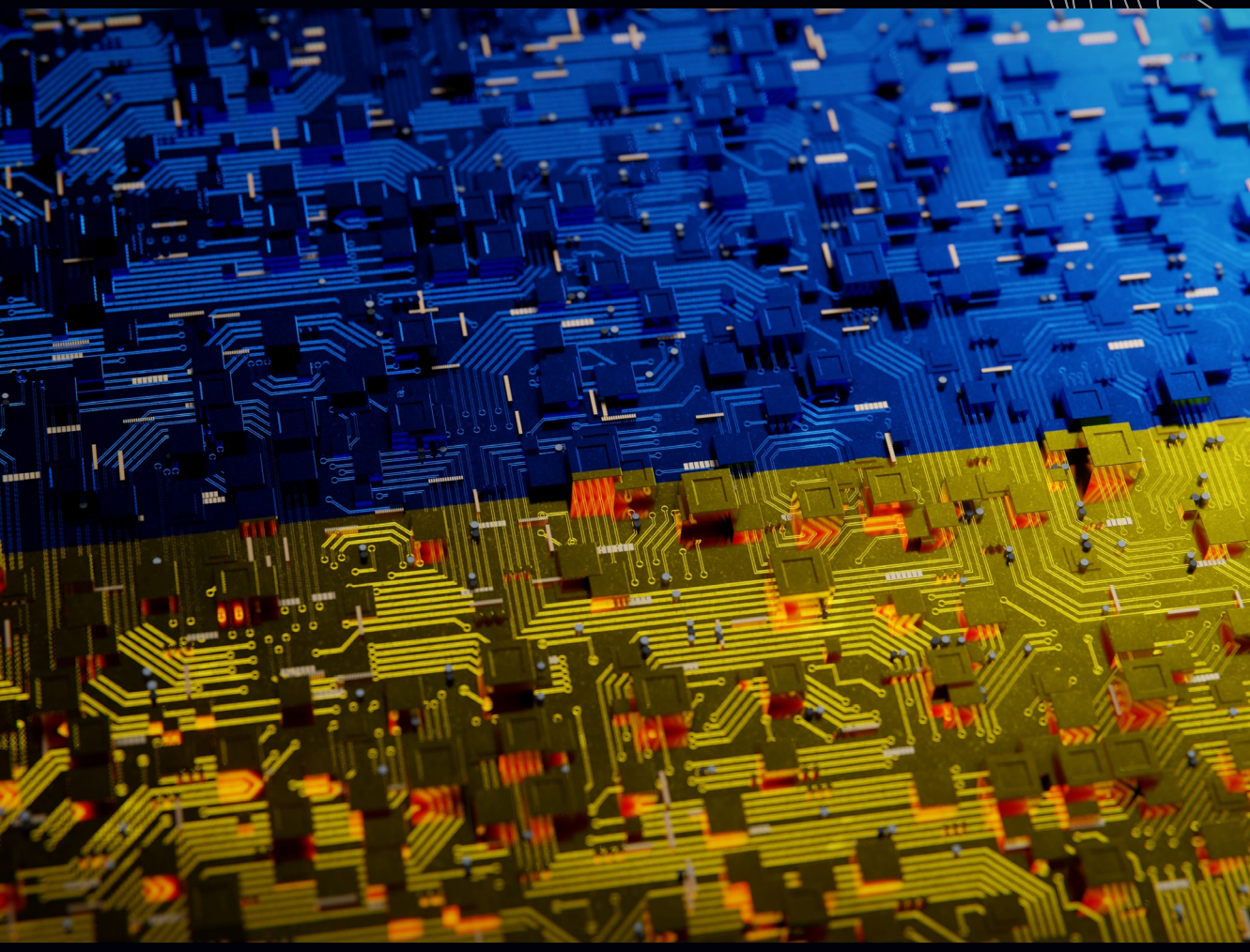
CYBER SECURITY - PARTNERSHIP BETWEEN DEFENCE, SOCIETY AND PRIVATE COMPANIES - LESSONS FROM UKRAINE

PROFESSOR MATTHEW WARREN,
DR ADAM BARTLEY AND PROFESSOR AIDEN WARREN

AUSTRALIAN ARMY RESEARCH CENTRE
/ Australian Army Occasional Paper No. 35



SERVING THE NATION

ARMY.GOV.AU

CYBER SECURITY - PARTNERSHIP BETWEEN DEFENCE, SOCIETY AND PRIVATE COMPANIES - LESSONS FROM UKRAINE

PROFESSOR MATTHEW WARREN,
DR ADAM BARTLEY AND PROFESSOR AIDEN WARREN

AUSTRALIAN ARMY RESEARCH CENTRE
/ Australian Army Occasional Paper No. 35

ISSN (Print) 2653-0406

ISSN (Digital) 2653-0414

DOI: 10.61451/2675149

All enquiries regarding this publication should be forwarded to the Director of the Australian Army Research Centre.

To learn about the work of the Australian Army Research Centre visit
https://researchcentre.army.gov.au

Cover image: Technology background with national flag of Ukraine by HTGanzo.
(Source: Adobe Stock)

/ CONTENTS

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ ACKNOWLEDGEMENTS

RMIT University's Centre for Cyber Security Research and Innovation thanks the Australian Army Research Centre and the Department of Defence for sponsoring this project.

We express our sincere thanks to all the participants in Estonia, Lithuania and Latvia and online. In particular, we are grateful for the support provided by our partners and affiliates in these countries, especially the NATO Cooperative Cyber Defence Centre of Excellence, Estonia, NATO's Strategic Communications Centre of Excellence, Latvia, and Mykolas Romeris University, Lithuania, for hosting and facilitating our workshops and interviews in Europe. We are also grateful for the project support of the Estonian, Latvian, Lithuanian and Ukrainian governments and their military, as well as the support of Australian Defence Force (ADF) representatives in Europe.

We would like to thank the following individuals:

- His Excellency Jaan Reinhold, Ambassador of the Republic of Estonia to the Commonwealth of Australia
- His Excellency Margers Krams, Ambassador of the Republic of Latvia to the Commonwealth of Australia
- His Excellency Darius Degutis, Ambassador of the Republic of Lithuania to the Commonwealth of Australia
- His Excellency Vasyl Myroshnychenko, Ambassador of Ukraine to the Commonwealth of Australia
- Zivile Krisciune, Senior Business Development Manager, Australian Trade and Investment Commission
- Professor Marius Laurinaitis, Mykolas Romeris University, Lithuania.

This research report was produced by RMIT University staff: Professor Matthew Warren, Dr Adam Bartley, Professor Aiden Warren, Dr Malka N Halgamuge, Valerii Paziuk, Tom Saxton, Meredith Jones, Amal Varghese, Lee-ann Phillips and Laki Kondylas.

Acknowledgement of Country

RMIT University acknowledges the people of the Woi wurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledges their Ancestors and Elders, past and present.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ ABSTRACT

The Russia–Ukraine conflict demonstrates the significance of cyber operations in modern warfare. Russia's continued cyber attacks against Ukraine have truly tested the strength of the defensive cyber capabilities of the Ukrainian government, military and critical infrastructure. This has led to Ukraine formulating and executing an agile cyber defence strategy that includes strong public–private partnerships, vocal international support, and technological innovation. This strategy has helped Ukraine maintain the effectiveness of its military operations.

This occasional paper examines the lessons learned from the Russia–Ukraine war and from Ukraine's cyber defence, and how these lessons can be utilised by the Australian Army to further build its own cyber operations. The paper explores how Ukraine's military has integrated commercial cyber capabilities into its warfare strategy, and it highlights the important role that multinational technology organisations and private sector partnerships play in building military cyber capabilities. The paper also considers Ukraine's approach to training frontline military personnel in cyber awareness and equipping them to operate effectively in difficult and opaque digital environments.

For the Australian Army, the Russia–Ukraine conflict provides valuable lessons on the need to build cyber capability and resilience, strengthen partnerships with public organisations and private industry, and build a whole-of-society approach to cyber operations.

/ EXECUTIVE SUMMARY

Increasingly sophisticated cyber threats and attacks have become an ever-present security challenge faced by all nations. The Russia–Ukraine war underscores the complexity of warfare with which nations and states must now contend. Ukraine's experience of modern warfare illustrates the intrinsic value of public–private partnerships and the positive role of wider society in mitigating and deterring cyber attacks.

The Russia–Ukraine conflict is being fought on a global stage, with the world watching intently as to how Ukraine handles the cyber war that is being waged against it. This conflict provides us with a 'live' case study of the execution of cyber warfare strategy as Russia deploys integrated cyber operations and engages citizens, hackers, and state and security services groups to achieve its military objectives. Sophisticated cyber operations and military attacks against Ukraine's critical infrastructure and wider society have been deployed with devastating results. Cyber espionage, data theft, vulnerability exploitation, and intelligence gathering have been used by Russia in ways that show the sophistication of Russia's cyber capabilities and the evolving and adaptive nature of the cyber threat environment.

The Ukrainian experience illustrates why it is important to understand the conditions and nuances of cyber warfare and to build cyber resilience. How can nations protect themselves against these increasingly sophisticated and innovative cyber attacks?

The response of the Ukrainian government in dealing with the intense cyber campaign it faced has been a success. Russia's ongoing cyber warfare campaign has had only minimal impact on the overall war. However, it has also been suggested that Ukraine's success in this area pre-dates the war and can be attributed to its lengthy exposure to Russian cyber attacks for many, many years and the robust cyber defence strategy (and accompanying capabilities) that has been built over time. While this prolonged exposure plays a part in Ukraine's successful defence, it minimises the in-depth approach the Ukrainian government has taken to developing the nation's cyber capabilities and resilience. The government has worked long and hard to develop 'the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources'.[1]

In addition to the Ukraine government's concerted efforts, the wider Ukraine society and strong cyber volunteer networks have been instrumental in building Ukraine's substantial cyber defence approach. The astute mobilisation of civilians with advanced technology skills and experience with cyber initiatives (e.g. the IT Army of Ukraine) has provided the nation with a level of resilience that is both extremely broad and deep. This mobilisation has enabled crowd-sourced information gathering, defensive cyber actions, retaliatory cyber attacks, and in-depth national involvement in cyber security. Together the Ukranian government, military and populace have developed a cyber warfare defence strategy that adopts a whole-of-society approach to protect the country where it is threatened by continued cyber hostilities.

Consequently, regardless of the enormous scale and high-level sophistication of Russia's cyber warfare operations, the impact of these operations has been curtailed as a direct result of Ukraine's whole-of-society cyber warfare response. This raises important questions about the effectiveness of cyber warfare as an instrument of modern conflict in the face of a robust strategic defence. While it is true that cyber attacks have caused some economic and operational disruption in Ukraine, such attacks have not caused significant damage to Ukraine's command and control structure, its military operations, its critical infrastructure, or its cyber resilience.

The insights from this paper drawn from the Russia–Ukraine conflict are designed to provide a foundational understanding of how we can anticipate, withstand, recover from, and adapt to the ever-changing cyber threat landscape.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ DEFINITIONS

APT	Advanced persistent threat—a stealth cyber actor with sophisticated capabilities that is usually state sponsored
AWS	Amazon Web Services
Bot	A program that performs automated tasks. In a cyber security context, a malware-infected computer that carries out tasks set by someone other than the device's legitimate user
Botnet	A collection of computers infected by bots and remotely controlled by an actor to conduct malicious activities without the user's knowledge, such as to send spam, spread malware, conduct denial of service activities or steal data
C4	Command, control, communications and computers
CERT.UA	Computer Emergency Response Team of Ukraine
CERT.LV	Computer Emergency Response Team of Latvia
Cyber resilience	The ability to effectively and efficiently adapt to disruptions caused by cyber security incidents while maintaining continuous operations
Distributed denial of service (DDoS)	Distributed denial of service campaigns are designed to disrupt or degrade online services such as website, email and domain name services. This can be through hacking, bandwidth overload and/or disruption of processing resources
Disinformation	False or inaccurate information is spread deliberately to manipulate the opinions and actions of others
FSB	Russian Federal Security Service (Federalnaya Sluzhba Bezopasnosti)
GRU	Russian military—Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Glavnoe Razvedyvatel'noe Upravleniye)

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

IT Army	Ukrainian IT Army. The IT Army comprises a diffuse set of volunteer hackers working in collaboration with officials from Ukraine's defence ministry to target Russian infrastructure and websites
KGB	Committee for State Security (Komitet Gosudarstvennoi Bezopasnosti) during the final years of the Soviet Union (now the FSB)
LEO	Low earth orbit
Malware	Malicious code that, once implanted, can be used to access information systems and control, steal, or hold to ransom (among other things) a system
Misinformation	False or inaccurate information spread without malicious intent. However, the effects of misinformation can still be harmful
Phishing	A technique used by criminals/attackers to trick a person into handing over sensitive/personal information, usually for the purposes of stealing information, money, or identity
Sandworm	Russian APT group, also known by vendors as IRIDIUM, VOODOO BEAR, BE2, UAC-0113, Blue Echidna, PHANTOM, BlackEnergy Lite, and APT44
SBU	Ukraine Security Services (Sluzhba bezpeky Ukrainy)
SSSCIP	State Service for Special Communications and Information Protection
SVR	Foreign Intelligence Service (Sluzhba Vneshney Razvedki), Russian spy agency
UAV	Unmanned aerial vehicle
USAID	United States Agency for International Development. USAID is the US government agency that leads international development and humanitarian assistance efforts to partner countries
WAAP	Web app and API protection

/ INTRODUCTION

Ukraine gained independence after the collapse of the Soviet Union in 1991. It then veered between seeking closer integration with Western Europe and being drawn into the orbit of Russia, a country which sees its interests as threatened by a Western-leaning Ukraine.[2] After the November 2013 to February 2014 Maidan Uprising in Ukraine, which led to the ousting of Russia-leaning President Yanukovych, the government of Petro Poroshenko developed action plans and the underlying architecture for new e-government services.[3] In 2014, Russia seized the Crimean Peninsula from Ukraine, and armed insurgent groups occupied parts of eastern Ukraine. The Russian army eventually launched a full-scale invasion of Ukraine in February 2022.

Following Russia's annexation of Crimea, there was an increase of cyber attacks against Ukraine's critical infrastructure systems, leading one analyst to call Ukraine a testing ground for Russian cyber capabilities.[4]

Ukraine had transformed during the nine years to 2022, primarily in the cyber area and via the growth in national and international partnerships. This capability is illustrated in the cyber operations targeting critical Ukrainian infrastructure, including media, government and military networks in the years and months preceding the military invasion.

Russian-affiliated hackers, who operate under Kremlin and Russian military intelligence command, launched major attacks which disrupted elections, defaced government websites, deleted state system data and threatened to cause extensive disruptions.[5] There were also cyber attacks against Ukraine's regional power grids in 2015 and the Kyiv transmission system in 2016, and the NotPetya malware attack in 2017, which demonstrated an ongoing plan to damage Ukraine's cyber infrastructure and reduce public and institutional resistance.[6]

The Ukraine Security Services (SBU) cyber department documented 15 major cyber security incidents each day in 2023 which occurred simultaneously with missile attacks to create extensive disruptions in critical infrastructure.[7] In 2023, 3,000 cyber security attacks were recorded 3,000 cyber security attacks against Ukraine's critical infrastructure, including military and civilian assets. One of the planned outcomes of the cyber security attacks was to reduce Ukraine's national capabilities and contribute to eroding public support for the Ukrainian government.[8] [9]

Many felt that an organised cyber security offensive would be capable of paralysing Ukraine's command and control and logistics. The actual cyber impact has been less destructive.[10] As Nick Beecroft has written, 'Russia's much-feared cyber war has failed

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

to materialise the way that many experts anticipated it would'. Attempts to bombard the country with cyber attacks failed to deliver the catastrophic blow that Russia required.[11] While 'nowhere on the planet has ever been targeted with more specimens of data destroying code in a single year' than Ukraine, wrote Wired's Andy Greenberg, the operations revealed a much less sophisticated arsenal of cyber weapons and more 'quick, dirty, relentless, repeated, and relatively simple acts of sabotage'.[12]

Tracking Ukraine's successful weathering of Russia's cyber warfare onslaught reveals the significance of international partnerships, assistance and, in some cases, pressure to radically alter government information technology (IT) and cyber security processes, regulations, operations and, fundamentally, culture. From the start of the second invasion, major multinational corporations were in contact with Ukrainian interlocutors and establishing what would become durable partnerships of major cyber assistance. Microsoft, for instance, was able to provide a patch to mitigate a new type of malware attack—attacks aimed at Ukrainian military institutions and Ukrainian government agencies with the aim of weaponising victims' computers and using them as part of distributed denial of service (DDoS) campaigns.[13] A team from Amazon Web Services (AWS) contacted Ukrainian representatives on the day of the invasion, offering facilities to securely transfer key government data to the cloud with solutions architects already in the country.[14]

The Baltic states of Estonia, Latvia and Lithuania have had a similar journey to that of Ukraine, being formerly part of the Soviet Union, and they have similarly sought to transform their economies and societies. The Baltic states are very supportive of Ukraine; for instance, the Estonian government has been particularly supportive of Ukraine in terms of helping with their national digital transformation,[15] and Lithuania has provided support through national crowd-sourcing funds for drone purchases for Ukraine.[16]

Despite the critical role partnerships have played in strengthening Ukraine's defence against Russian cyber aggression, there has been no systemic study of these partnerships and their broader implications for military force readiness, especially in key areas such as cyber security. Understanding how Ukraine's government, military, private sector, and international technology partners collaborated in response to unprecedented cyber threats is essential for shaping future cyber security strategies in allied nations.

The Australian Army, like many modern defence forces, is increasingly reliant on cyber security capabilities to support military operations, logistics, and national security. The Ukraine war provides a real-world case study on how partnerships between society, industry and government work.

/ METHODOLOGY

This study employs a qualitative research design structured in three key phases to examine the role and effectiveness of cyber partnerships in Ukraine. The research integrates multiple sources of data, including open-source intelligence, literature review, expert interviews, and policy analysis, to develop a comprehensive understanding of cyber security defence collaborations.

Background Research and Data Collection

The first phase of the study involved an extensive review of available information and a literature review, as well as publicly available datasets, to map the key actors and contributions of cyber security professionals, national technology firms, and cyber civil society organisations in mitigating Russian cyber aggression. This stage provided foundational insights into Ukraine's evolving cyber security landscape, identifying how public–private and international cyber security partnerships were established and operationalised.

Key Informant Interviews and Expert Workshops

The second phase of the research centred on primary data collection through semi-structured interviews and expert workshops conducted in the Baltic states of Estonia, Latvia and Lithuania. The interviews were held with a number of key stakeholders, including cyber security specialists, industry representatives, and government and military representatives from Estonia, Latvia and Lithuania and Ukraine.

The research also included 15 key informant interviews to achieve a balanced understanding of cyber resilience contributions from public and private sectors. The three workshops enabled knowledge sharing between participants which produced comparative findings about cyber defence approaches in Ukraine and the Baltic states. The team conducted additional briefings with senior government and military personnel to gain strategic context and background information. These briefings provided detailed insights about the achievements and operational challenges and strategies of Ukraine and how partnerships were developed.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

Policy and Data Analysis

The final phase required policy analysis and synthesis of data obtained from the interviews, workshop discussions, and official documents. The analysis extracted useful information to develop evidence-based policy recommendations which would improve cyber collaboration in Ukraine and beyond. The research combined qualitative insights with policy analysis to conduct a systematic evaluation of cyber partnerships regarding Ukraine.

The findings of the research offer strategic guidance for strengthening international cyber cooperation and informing military and civilian cyber security initiatives, including those relevant to the Australian Army.

The project adhered to stringent ethical standards and was approved by the Australian Departments of Defence and Veterans' Affairs Human Research Ethics Committee. All participants were informed about the purpose of the research, the confidentiality measures in place, and their rights as participants before providing their consent.
The research was completed in December 2024.

/ OVERVIEW OF UKRAINE SITUATION

The transformation of Ukraine's cyber capabilities and governance, and the responses to Russian cyber aggression from 2014 to 2022, provides a unique experience for a country to develop its national capability. From an industry and partnership perspective, the immediate post-2014 phase showcased a government beset by inexplicable bureaucracy, pushback, and confusion. Many countries post Soviet Union independence had to deal with challenges of corruption and poor bureaucracy.

The problems threatened to discourage future donor backing, which demonstrated the requirement for improved inter-agency coordination, better planning and proactive donor and domestic enterprise engagement. This meant that progress was hindered by systemic issues including financial constraints, fragmented coordination, and limited public–private collaboration.[17]

The context in which these challenges have been overcome, or limited, in the reform and then development of the nation's cyber capabilities highlights several contributing factors. At the national level, the determination to push back against Russian aggression provided a catalyst for international support that came in the form of financial aid, cyber training and upskilling, free access to software licences, and other programs and technologies.
A corresponding aspect was the openness and ability to accept foreign aid and technical advice, and to respond to Western demands for reform and transparency. But perhaps most significantly, the strategic determination to achieve full membership of both the EU and NATO underscored the parameters for development and reform going forward, specifically deconflicting and aligning Ukraine's policies, laws and regulations with EU governance mechanisms.[18]

Indicatively, key partnerships with the US, the EU and NATO have been critical to this societal and governmental transformation. Prior to 2020, accounts of US support highlighted over US$2.5 billion in military aid to Ukraine, focusing on the hardware attributes of warfare.[19] However, much of this assistance has also included the development of the components of societal resilience, hardening the base for public–private partnerships, and civil society development. These efforts have included the deployment of advisers to help 'stabilise the financial sector and implement key reforms in partnership with the Ukrainian Finance Ministry and National Bank', support reforms on banking supervision, and address 'public sector debt management, infrastructure finance, and taxation'; increased support and access to finance for Ukrainian businesses through the European Bank for Reconstruction and Development and the Organisation

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

for Economic Co-operation and Development, as well as help in reforms to attract international investment; assistance in developing anti-corruption institutions within government; and expanded support for e-governance and procurement reform.[20] Other international examples include support from the United States Agency for International Development (USAID), and US authorities' contribution of US$37 million to cyber security management and advisory services to the Ukrainian government. These cyber challenges had led to a limited cyber attack response capability, a lack of public–private partnerships, and poor-quality of threat intelligence and cyber audits.[21]

In NATO, several contributions have sought to address inter-agency coordination, government planning and procurement, and international engagement. The NATO-Ukraine Command, Control, Communications and Computers (C4) Trust Fund agreement, signed in April 2015, for instance, has sought to modernise Ukraine's C4 structures and capabilities and facilitate their interoperability with NATO, with outcomes aimed at contributing to NATO-led exercises and Ukraine security development.[22]
The NATO-Ukraine Cyber Defence Trust Fund has helped develop Ukrainian technical capabilities, including an incident management centre 'for the monitoring of cyber security events and the establishment of laboratories to investigate cyber security incidents'.[23] Additionally, the NATO-Ukraine Logistics and Standardization Trust Fund was set up in April 2015 to reform the country's logistics system in line with NATO and increase interoperability through standards 'for the tracking and management of national military equipment and supplies'.[24] Meanwhile, NATO's Building Integrity (BI) Programme with Ukraine has sought to strengthen integrity, transparency and accountability in Ukraine's defence and security sector and reduce the risk of corruption.[25]

These initiatives illustrate the depth of international collaboration with Ukraine, and they also highlight the origins of the new public–private partnership model that has come to define Ukraine's current cyber approach. This became the basis of the Ukrainian 2016 Cyber Security Strategy.[26] Its principles encompassed shared goals, a commitment to the development of modern critical infrastructure (allowing private solutions to integrate seamlessly), and the deepening of trust built through transparency and reform.[27]
In practice, the first objective was the 'immediate establishment of a national cyber security system as an integral part of the national security of Ukraine'.[28] Public–private partnerships sat below this as fourth on the list of principles of vital interests of the state with 'extensive cooperation with civil society for cyber security and cyber defence' earmarked for strategic engagement. This development coincided with emphasis on the 'formation and operational adaptation of state cyber security policy on the cyber space development, achieving compatibility with the relevant EU and NATO standards'.[29]

Following this, the 2017 Law on the Basic Principles of Ensuring Cyber Security of Ukraine deepened the government's commitment to addressing the challenges of organisational foundation, which had previously lacked legal definition and nuance. The law designated

'powers and responsibilities of state agencies, enterprises, institutions, organizations, individuals and citizens, the basic principles of coordination of their activities, as well as basic terms in the field of cyber security'. In parallel, the government telegraphed its seriousness about tackling the former patronage networks that defined government contracts and contributed to corruption.[30] For instance, several cases against high-profile corruption in the defence sector, where an estimated 30 percent of any foreign military purchase was misappropriated, helped to counter claims that Ukraine's reform had stagnated.[31] But more importantly, the 2017 law defined the national cyber security system and coordination of cyber security actors.[32] Proposals of experts from the EU and NATO were incorporated, with close cooperation with the commercial sector and civil society a common aim.

Still, by 2020, Ukraine's cyber strategy revealed a partnership model defined more by its individual parts than by its whole. The 2021 cyber strategy, for instance, had firmly focused on deepening the European model through institutional, technological and cultural changes; however, these reforms were still considered to be based on 'outdated standards of cyber security'[33] and they demonstrated limited cyber risk awareness.[34] Russia's cyber aggression continued to target Ukrainian critical infrastructure, ensuring that the government's strategic priority remained deterring and preventing cyber threats, with some accounts highlighting the failure of this principle after 2022.[35] But by this stage, Ukraine had established clear priorities in its cyber strategy focused on resilience (and the beginning of an approach to supporting critical national infrastructure). It was also prioritising the 'development of communication, coordination, and partnership between cyber security actors at the national level' corresponding with 'strategic relations in the field of cyber security with key foreign partners, especially with the European Union, the United States, and other NATO member states and international organisations'.[36]

It is worth noting, too, that the nation's cyber challenges had become much more transparently identified. Differentiated units and technologies among national electronics infrastructure continued to plague the government, and 'insufficient and unsystematic cyber protection measures of critical infrastructure, limited inter-agency coordination and capacity in combating cyber threats of military and criminal origins, and inadequate coordination, cooperation, and information exchange among cyber security entities' were also ongoing problems.[37] However, far from being outdated in terms of standards of cyber security, the nation's interface between cyber threats and capabilities had become clearly nuanced, as formerly systemic challenges were untangled in strategy documents, actions, plans and national policy.

This growing resilience is highlighted by the expansion of the Computer Emergency Response Team of Ukraine (CERT.UA) and development of the nation's capacity-building program among regional cyber security centres directed by the SBU to respond to Russian cyber threats. CERT.UA improved its integration and analysis of data on cyber incidents and expanded information sharing among state bodies and private sector owners of critical infrastructure, to which it provided services.[38] Additionally, the Cyber Security Situational Awareness Center of the SBU created the Malware Information Sharing Platform—Ukrainian Advantage (MISP-UA), deepening information sharing to include smaller businesses. In recognising the cyber capacity challenges in the private sector, as well as those in the critical infrastructure category, CERT.UA has spearheaded organisation of cyber protection workshops and conferences across law enforcement agencies and foreign and international organisations, often in cooperation with European partners.[39]

Additional changes in 2022 to laws to 'strengthen capabilities for cyber protection of state information resources and objects of critical information infrastructure' by the State Service for Special Communications and Information Protection (SSSCIP) has sought to embed measures of cyber security in the private sector, including through the creation of cyber defence units.[40] Some pushback has occurred against what is seen as the over-centralisation of power and control of SSSCIP, and the government has responded by reviewing relevant Ukrainian legislation. However, the broader picture up to this point has revealed a slow-paced institutional transformation, partly because of the broad-based reforms required across the key security, judicial and economic sectors. The larger reform initiative that began in 2023, by contrast, has worked to further build trust in public–private partnerships and has introduced digitalisation processes for engagement. The Ukrainian parliament has also passed new laws to provide war insurance for investments by both international companies and Ukrainian companies, and is communicating with the World Bank's Multilateral Investment Guarantee Agency (MIGA), the U.S. International Development Finance Corporation (DFC) and other donors for a US$100 million reinsurance scheme for its Export Credit Agency.[41] These changes have ignited debate about Ukraine's robust start-up environment and have pushed partnerships to begin envisioning collaboration beyond the current wartime setting.

Individual countries have also assisted Ukraine. Estonia, renowned for its global leadership in e-government through the Estonian e-Governance Academy, is spearheading the EU-funded project Digital Transformation for Ukraine (DT4UA) (€17.4 million).[42] This project aims to enhance the efficiency and security of public service delivery, ensuring better access for citizens and businesses in Ukraine. It also focuses on providing swift responses to wartime needs and strengthening daily governance.[43]

In sum, the experience of Ukraine's cyber governance development should be viewed as a versatile and pragmatic approach to building cyber resilience, international partnership, and the capacity for critical cyber attack response. Ukraine has learned over time and has improved its cyber resilience and cyber capabilities to their current state, but there are lessons that have been learned, these being the need for public–private cooperation reforms and a cultural shift towards openness and collaboration.

Public–Private Cooperation Reforms

The Ukrainian government took decisive action to tackle corruption and inefficiency in defence procurement, which demonstrated its commitment to transparency and accountability to both domestic and international audiences. The trust established by these reforms made private companies, including international technology firms, more likely to work with the Ukrainian government because it minimised the risk of resource misuse and reputational damage.

1. Institutional resilience created a collaborative foundation

US and EU aid supported the stabilisation of Ukraine's financial systems, modernised infrastructure and introduced governance reforms. These changes not only strengthened the state's capacity to manage crises but also demonstrated a commitment to long-term modernisation and reliability. Private companies often hesitate to collaborate with unstable or poorly governed systems, but these reforms mitigated those concerns, and Ukraine's ability to attract and sustain private sector engagement such as through technology sharing, advisory services, and operational partnerships was significantly enhanced.

2. Cyber capability enhancements enabled shared responsibility

Initiatives like the NATO-Ukraine Cyber Defence Trust Fund helped build technical capacity (e.g. incident management centres and cyber security laboratories) that created the infrastructure necessary for private sector integration, as private companies often provide expertise, tools or services to complement state capabilities. The platform that emerged allowed government agencies and private firms to share intelligence, respond jointly to incidents, and coordinate resources effectively.

3. Digital transformation enabled dual-use platforms

Efforts to modernise Ukraine's digital governance (e.g. e-governance reforms) enhanced the country's ability to manage resources and coordinate activities digitally. Many of these systems were designed to be dual use, benefiting both civilian and defence sectors. The private sector could innovate within these frameworks, such as providing cyber security solutions for critical infrastructure. This dual-use infrastructure bridged the gap between public governance and private innovation, making it easier to build integrated cyber defence mechanisms.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ UKRAINE INDUSTRY ENGAGEMENT

The cyber warfare component of Russia's invasion of Ukraine has warranted investigation of the roles of the private sector and the provision of critical communications technologies and capabilities.[44] For governments, public–private partnerships are strategic vehicles for innovation, growth, access to expertise, and access to the broader resources and technologies of the private sector. Additionally, the role of the private sector in the ownership of national critical infrastructure (defined by NATO Allied Command Operations as 'nation's infrastructure, assets, facilities, systems, networks, and processes that support the military, economic, political, and/or social life on which a nation … depends'[45]) requires joint ownership of the threats facing the nation or it risks fragmented resilience.
Put differently, a government's ability to respond to and recover from cyber threats at speed is intricately tied to private sector preparedness and the systematic interaction between the public and private sectors.[46] In short, an effective cyber defence strategy and model for partnerships combines a dynamic of pragmatic governance, efficient coordination, responsibility sharing and, in Ukraine's case, strategic international industry engagement.

Fig 1 - A volunteer makes camouflage nets for Ukrainian soldiers, 09 January 2024. (Source: Elena Tita / the collection of war.ukraine.ua)

The gradual development of Ukraine's cyber security capabilities, as mentioned previously, defines a scope of wide industry and civil society engagement. These public–private collaborations have been varied and reactive to the immediate challenges of aggressive Russian cyber activities, making a versatile, albeit ad hoc, approach to partnerships.
It is worth pointing out that by 2022, Ukrainian government systems which had transformed through close collaboration with NATO, US and EU programs had become more compatible with broader Western systems and C4 modernisation efforts and, significantly, more exposed to networks of industry decision-makers and civil society facilitators that have participated in and around NATO and other EU projects.[47] This set the background for key partnerships at the beginning of the second invasion of Ukraine. The early example of the Microsoft Threat Intelligence Centre's assistance in disrupting the Russian malware attack on Ukraine's critical infrastructure is perhaps the most widely known example.[48] Another is AWS's facilitation of services to transfer government data to the cloud.[49] Hundreds of partnerships exemplify Ukraine's response; some of the key partnerships are mentioned here.

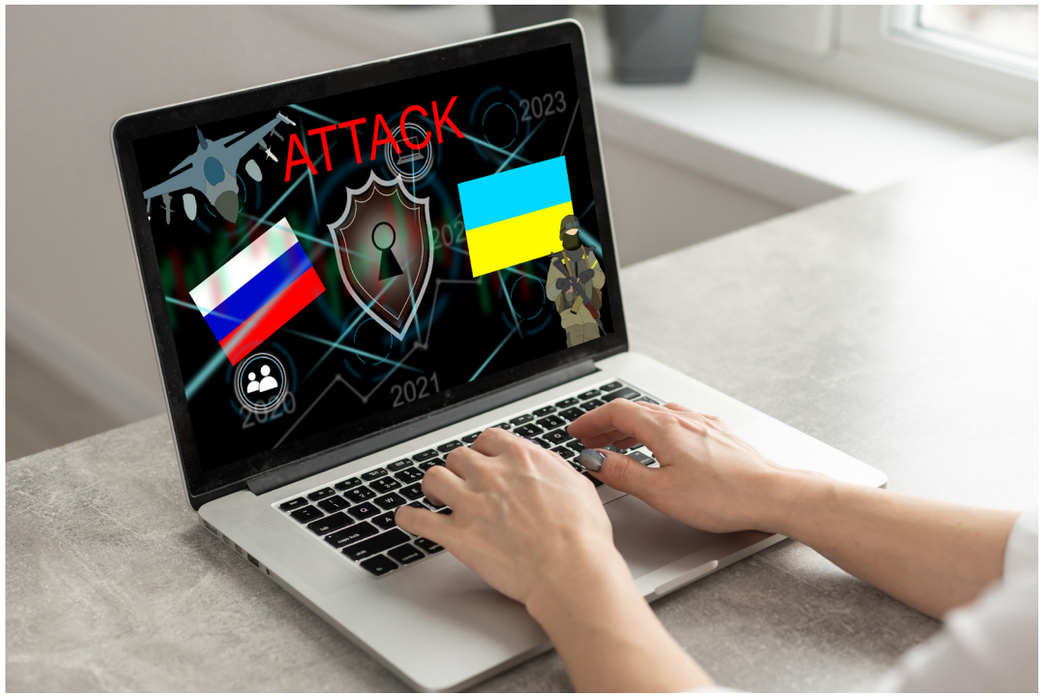


Fig 2 – Cyber security concept – (Source: Adobe / Angelov).

Russia's cyber capabilities and the versatility in their deployment, as well as the range of actors that it has employed, has in many ways defined its framework of engagement. Following the Ukrainian Maidan protests in 2013, Russian activities focused on DDoS campaigns against critical infrastructure such as national security agencies and media

outlets. In May 2014, the GRU-linked hacking group Cyber Berkut carried out a cyber attack on the nation's Central Election Commission, disrupting key network nodes and other system components, albeit with minimal impact.39 From 2015 onwards, however, Russian cyber activities, operating out of the GRU, the FSB and the SVR, escalated and expanded with a focus on critical infrastructure.39 On 23 December 2015, malware was used to infiltrate the control systems of the regional electricity hub Prykarpattya Oblenergo, shutting down 30 substations and electricity for 230,000 residents.[50] The trend lines of Russian attacks also displayed a growing sophistication. On 6 December 2016, another attack deploying malware that impacted government websites delayed government budget payments.[51] In July 2017, GRU-linked hacker group APT44 Sandworm deployed the NotPetya virus, severely damaging Ukrainian infrastructure while targeting the 'financial system, government networks, energy companies, and even the radiation monitoring system at the Chernobyl Nuclear Power Plant'.[52]

Whereas the pre-invasion period 'saw a broad based cyber security attack significant reliance on malicious code, phishing, and malware distribution, indicating a broad-based strategy to probe and exploit vulnerabilities across multiple fronts in the Ukraine', the 2022 invasion and post-invasion contexts have revealed a more targeted and defined approach to destructive attacks. For instance, the Viasat satellite attack, launched just prior to the invasion, was a highly coordinated operation using 'zero day' malware to disable some Ukrainian military communications and disrupt critical communication channels across Europe.[53] As noted at the time by Viktor Zhora, the deputy head of Ukraine's State Service of Special Communications and Information Protection, 'It was a really huge loss in communications in the very beginning of war'.[54]

The approaches taken by Russia to disrupt Ukrainian partnerships have also highlighted the symbiotic relationship between Russian state and private interests and the focus, beyond traditional destructive malware attacks, of its cyber activities.

Russian state hackers who primarily target foreign secrets have started using ransomware to hide their espionage operations using methods that combine criminal tactics with state objectives.[55] For example, the implementation of ransomware as a service (RaaS) represents a major advancement in cyber crime operations.[56]

The line between nation-state and criminal actors is increasingly blurry as nation-states turn to criminal proxies as a tool of state power, then turn a blind eye to the cyber crime perpetrated by the same malicious actors.[57] This approach blurs the line between state-based hacking groups and criminal groups and allows the Russian government not to be held accountable for hacking incidents as they are undertaken by criminal gangs.

The broad-ranging threat of Russian cyber actors and their capabilities raises important questions about the capacities of states like Ukraine (or potentially Australia) to deter, repel or respond in kind and at scale. At the beginning of March 2022, Ukraine suffered

from several gaps in the cyber skills, capabilities and networks needed to defend itself from cyber attacks. In the 2020 National Cyber Power Index, Ukraine was classified as having limited capability.[58] In 2018, its development capacity—in terms of the ability to apply cyber security measures, provide technical expertise and provide upskilling for cyber professionals—was the lowest component of the country's cyber security index.[59]

Fig 3 - Civilians practise firing rifles. Free rifle courses for civilians were organised by the Rifle Training Center 'The First' in Zaporizhzhia. 31 March 2024. (Source: Elena Tita, https://war.ukraine.ua)

Following the 24 February 2022 Russian invasion of Ukraine, Ukraine had to increase its cyber capabilities. This has warranted the creation of civilian hacker corps, loosely defined by the name IT Army of Ukraine, to pool capabilities in the service of responding to and degrading, where possible, Russian IT capabilities. Some have styled the structure as a cyber militia, identifying the group as a state proxy, albeit with limited oversight. One argument is that they are likely 'control[led] by objectives lists'—'that is, the state in question exercises control over the cyber militia's activities by publishing lists of specific objectives'.[60] Others suggest they are less likely to play a combat role, but rather contribute by offering support for the SBU and Ministry of Defence.[61] Examples of Ukrainian civilian hacking successes, however, suggest that the answer is both. In April 2022, members of the IT Army hacked Russia's Chestny Znak food and logistics traceability system using a DDoS attack, disrupting perishable foods sales nationally over four days. The government

was required to relax policies on food sales to resolve the issue.[62] In another example, hackers gained access to a state TV channel during prime time to broadcast messages in support of Ukraine.[63] These Ukrainian ad hoc groups have delivered important services through their operations which target Russian government and societal facilities in addition to their direct cyber attacks against Russian targets.

As Kaushik has also remarked, these volunteers provide a critical function in building trust between the government and the private sector.[64] Ukraine has been very successful in defending against Russia's cyber aggression. This achievement was based on the Ukrainians' own capabilities, partnerships with Western IT organisations, and the ability to use volunteer groups such as the IT Army of Ukraine. The speed with which Ukraine's cyber capability was developed was very rapid, which could result in problems—for example, how to integrate non-military units into military operations, how to coordinate dispersed global volunteers, and how to implement effective security vetting.

While there is some interaction between the cyber volunteers and the SBU, among other agencies, it is unclear whether this amounts to a broader systemic cyber network. In some cases, hackers have been recruited directly into military roles, illustrating a transference of labour and skills into the defence sector.[65] It has also been noted that the government has sought to recruit technical expertise in IT through conscription and via professionals from the private sector 'volunteering their time and expertise on fields like incident response, building cyber resilient systems among others'.[66] Another example is the creation of a military CERT in 2024 focusing on the safeguarding of military and communications networks, which has expanded skilled labour needs. Ukraine's Deputy Defense Minister for Digital Development, Kateryna Chernohorenko, has remarked: 'We are constantly looking for new specialists to join our team'.[67] However, broader integration raises legal and security questions. These include issues of 'confidentiality/classified information screening, privacy, remuneration, command-and-control or co-ordination structures, legal status and responsibilities under national and international law, particularly in armed conflicts'.[68]

One solution is the Estonian model of the Cyber Defence Unit of the Estonian Defence League (EDL), a paramilitary organisation. In a non-combatant role, according to Kotliarov et al.:

> units might include education and training, professional support to public and private organisations (specifically, consultation on security measures, red-teaming, and implementation of tests on the security functions of information systems, threat, and other information intelligence), and support in investigation of incidents and restoration of functions, especially in times of emergency.[69]

The EDL was set up in 2007 and has been in operation for decades.[70]

For the time being, the civil-defence model for Ukrainian cyber defence is underdeveloped and under-institutionalised, leading to suggestions that an under-optimisation of resources and talent is occurring. In this regard, Ukraine faces a number of major challenges:

1. How to integrate civilian ad hoc organisations into current military operations
2. Once the war is over, how to transform civilian ad hoc organisations into a professional organisation
3. How to deal with the potential issue of insider threats from a large number of unknown online volunteers.

In terms of innovation, the Ukrainian government has also established the Brave1 platform as a source of seed funding for Ukrainian start-ups in defence industry platforms and for collaboration with domestic and international partners. The platform seeks to extend defence industrial reach among stakeholders while providing organisational and informational support for technology projects. This approach has been successful in the unmanned aerial vehicle (UAV) space, where it has had critical backing by the president while additionally responding to the urgent needs of Ukraine's war effort.
Joint ventures between Germany's Rheinmetall and Ukrainian Defense Industry focusing on the maintenance and repair of German-provided vehicles, and Türkiye's Baykar and three Ukrainian companies on UAVs showcase the current focus of the platform.[71] According to an official government press release, 20 further agreements and memorandums were signed in 2023 between Ukrainian and foreign partners at the International Forum of Defense Industries; however, not much information has been provided on what these arrangements are or what technologies they will develop.[72]
For the time being, the Brave1 seed funding remains small (US$25,000) compared to what start-ups require for development.

Internationally, Ukraine has benefited from regional forums like the Ukrainian Drone Defence Forum, London. This forum has been successful in placing leading Ukrainian drone manufacturers in touch with the UK defence industry trade association, and funding opportunities otherwise non-extant in a peacetime situation. For instance, the UK's allocation of £325 million to support British and Ukrainian drone manufacturing and to scale drone and electronic warfare production capabilities has contributed to a robust drone start-up capability that now supports around 200 companies in Ukraine.[73] Another example is the Eurosatory exhibition in Paris in June 2024, which saw Ukrainian Defense Industry (formerly Ukroboronprom) companies sign five agreements with Thales, Hexadron, Exail and Aequus. These agreements involved systems including electronic warfare, communications, navigation using Ukraine-made radars, military vehicles, and drones, with the French association GICA also signing a memorandum of cooperation with the Technological Forces of Ukraine Association.[74] With highly dynamic conditions on the

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

battlefield in Ukraine demanding ceaseless innovation—including, for instance, constant changes to hardware systems' software output, sometimes while units are operating systems in the field—these partnerships have proved critical.[75]

In the cyber space, the corresponding platform has become the Tallinn Mechanism, a consortium of 10 nations established in December 2023. Within this platform, Ukraine is prioritising, deconflicting and accelerating allied services, platforms and products for Ukraine cyber defence.[76] The Tallinn Mechanism offers a more streamlined approach to the provision of cyber assets, technology, knowledge and training, with a dedicated ambassador and financing being contributed through the Estonian embassy. The grouping is new, and it is unclear yet how it has contributed to Ukrainian cyber needs. However, the platform draws on earlier and ongoing examples of coordinated outreach programs and has likely been developed to formalise and manage these earlier efforts.

In 2022, Kyiv began leveraging civil society networks to draw influence and interest in its cause and to set up lines of communications from within the SSSCIP and Ministry of Digital Transformation. The Cyber Defensive Assistance Collaborative (CDAC), a volunteer group drawn from Western cyber security companies and organisations with wide links between governments (particularly the US and other major Western cyber entities), became a key conduit for Ukraine cyber needs. In Ukraine, CDAC discovered that its contacts grew quickly 'as more Ukrainian organisations expressed a need for improved threat intelligence capabilities, licenses, and training for cyber defense tools'.[77] According to CDAC, other participants have also contributed to the platform, including the Cyber Threat Alliance (CTA), to set up a threat intelligence management platform (ThreatQ) with the US firm ThreatQuotient to integrate call to action data through application programming interfaces. Other companies, such as Recorded Future and Mandiant, have begun sending their information to the platform as well, with input also from the Cybersecurity and Infrastructure Security Agency and the US Department of Homeland Security.

The foundation of Ukraine's digital transformation was laid before 2020. President Volodymyr Zelenskyy's vision of a 'state in a smartphone' was institutionalised through the creation of the Ministry of Digital Transformation in 2019, led by Deputy Prime Minister Mykhailo Fedorov. The ministry introduced a chief digital transformation officer (CDTO) system at all levels of government, ensuring decentralised and harmonised implementation of digital initiatives.[78]

The Diia ('Action' in Ukrainian) ecosystem became a crucial development when it launched in 2020 with its digital-first and mobile-first strategy. The Diia platform functions as an integrated system that provides digital identification alongside public services. Ukraine achieved a historic milestone by becoming the first nation worldwide to introduce a digital passport that holds equal legal value to physical documents, and the fourth European country to implement a digital driver's licence. The system enables automatic business registration through a streamlined process that takes only 10 minutes.[79]

The Diia platform is an example of global cooperation with funding and support from USAID, UK aid, the EU and other global partners.[80]

Diia has grown into a critical platform offering over 125 government services online and 30 services via its mobile app. In 2025, more than 14 million people in Ukraine are using the Diia ecosystem and its features.[81]

Transformation

The Diia platform allows civilians to report damage to property, claim assistance for displaced persons, and even contribute to national security efforts through the 'єВорог' chatbot, which enables users to share real-time intelligence on Russian troop movements. Other services include obtaining and cancelling 'internally displaced persons' (IDP) status, reporting damage to property, compensating businesses for employing IDPs, and participating in e-recovery programs. Diia stands as a powerful example of how Ukrainian digital infrastructure, developed through government–industry collaboration, can contribute to national resilience in both peacetime and war.

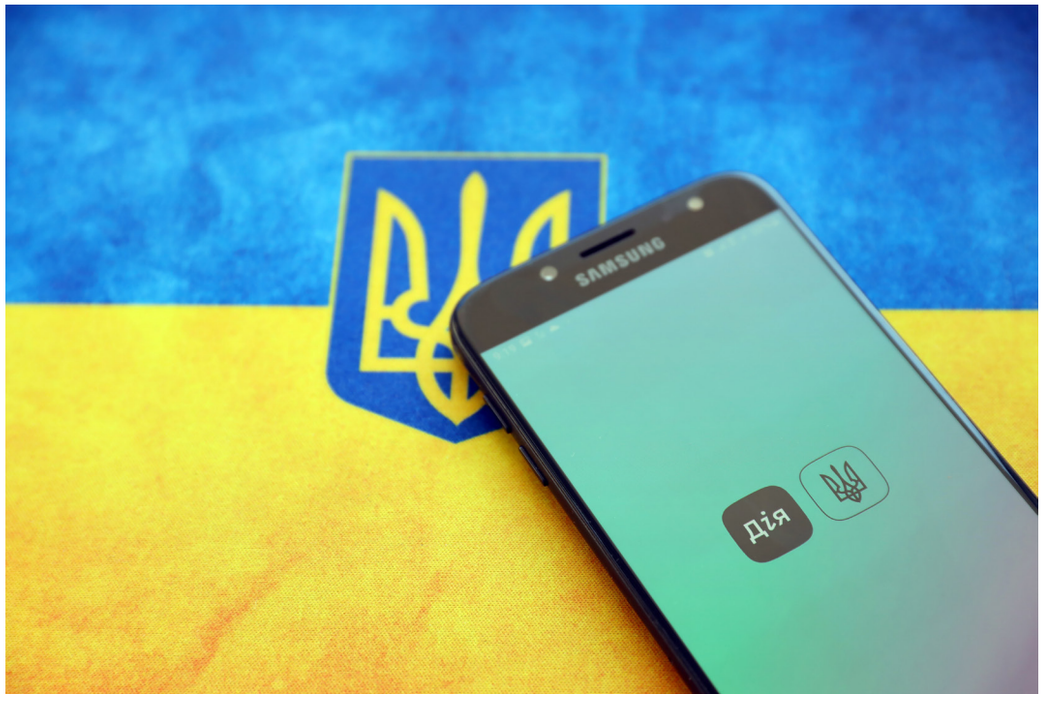


Fig 4 – TERNOPIL, UKRAINE - APRIL 24, 2022: Diia app on smartphone screen. Diya is a mobile application with web portal and a brand of e-governance in Ukraine. (Source: mehaniq41)

To overcome the cyber skills shortage, Ukraine has openly cultivated non-traditional volunteers for participation in often offensive activities against an adversary. In the days immediately following the Russian territorial invasion, the Ministry for Digital Transformation of Ukraine announced a call for the country's IT specialists to join the fight against Russia in cyber space.[82] The need to create a 'volunteer organisation' to help neutralise cyber threats was foreshadowed as early as 2016 in the National Cybersecurity Strategy, illustrating at the time the varied and systematic threats of Russian cyber capabilities.[83] The IT Army grew to more than 300,000 volunteers within days of its creation, providing immediate scaling for the government, and potentially the armed forces, otherwise unavailable during peacetime.[84]

/ BALTIC EXPERIENCES

Our workshops with stakeholders in Estonia, Latvia and Lithuania highlighted the direct vulnerability Russia's neighbours face to cyber attacks. These range from attacks such as DDoS campaigns and malware to information operations, cyber criminal activities, and espionage. The overview of the Baltic cyber situation reveals an ecosystem of attacks with increasing sophistication and response protocols illustrating that a strong relationship has grown between Ukraine and the three Baltic states in the larger conflict with Russia. Many in the Baltic states feel that their countries' fates are intertwined and, given the long history and experiences of occupation by Russia across centuries, fears have skyrocketed that, if Russia succeeds in Ukraine, the Baltic states may be invaded too.

The Baltic states maintain their position as essential centres for developing new cyber security solutions because they possess both state-of-the-art digital systems and extensive experience with cyber attacks. At the same time the Ukraine was being invaded, Estonia faced multiple and unprecedented waves of cyber attacks, primarily driven by pro-Kremlin hacktivist groups. The attacks against the Baltic states were largely DDoS attacks focusing on critical infrastructure, targeting government websites, educational institutions, the transportation sector, and media companies. [85]

Estonia

In 2007, Estonia was impacted by a national cyber attack from Russia. This attack was a coordinated DDoS campaign targeting Estonian government websites, the transportation sector, and media companies.[86]

In Estonia, the concept of 'total defence' was developed, with a constitutional role for civilians in the event of an attack against the state. This concept has underscored efforts to ready the state for both full-frontal and hybrid forms of attack. This includes greater funding for conventional and maritime forces and also, crucially, sectors where dual-use capabilities can be employed for asymmetric advantage within the cyber and psychological domains.[87]

Additional spending has been allocated to the volunteer National Defence League (NDL) for training, recruitment, and also information operations and cyber components. For instance, the NDL has established 'cyber units for military and civilian activities' and for training, exercises and innovation.[88] Such units are generally established in cyber civilian networks of occupation (private sector and academia) but also contribute where necessary to support police and other state institutions. There are also examples of international collaboration with Poland. The cyber unit has approximately 300 members,

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

with 50 percent female representation, and, with cooperation from the Ministry of Defence, has deepened public–private networks and response procedures.[89]

Estonia has become as a global leader in e-governance because it built its digital infrastructure through public–private sector partnerships that gained worldwide recognition. As Tomas Jermalavičius notes, 'cyber security is viewed as a pivotal element of future secure, safe, and trustworthy AI systems'.[90] This commitment underscores Estonia's leadership in aligning defence, commerce, and digital resilience.

Latvia

Latvia has also been the subject of an increasing number of serious cyber attacks from malicious actors. For example, major DDoS campaigns have been perpetrated against the Latvian Ministry of Defence and Ministry of Foreign Affairs, CERT.LV, and other major state institutions in transport, economics, finance, health and parliament. These incidents have been attempts to degrade systems, disrupt civilian and defence capabilities, and erode support for government.[91] As witnessed across Ukraine, Estonia and Lithuania, Latvia's cyber security apparatuses have increased, at times with international aid, in response to the rise of malicious cyber activities against the state, private sector and academia. At the beginning of Russia's 2022 invasion of Ukraine, Canadian NATO cyber units who were in Latvia at the time offered to help the nation with cyber threat hunting capabilities. Two years on, they have deepened their partnership with Latvian counterparts in a unique bilateral cyber development. Latvian CERT.LV units, with Canadian help, later found their systems and institutions infiltrated by 'a lot of third parties', leading one interviewee to quip that it wasn't 'if you find out you've been compromised, but when you find out you've been compromised'.[92]

The Latvian government has also been proactive in reforming legislation, addressing funding shortfalls in cyber security protections and skills development, and raising broader awareness. This has included growth in the number of CERT.LV professionals with a focus on IT critical infrastructure, with stronger communication between CERT.LV and the Ministry of Defence.[93] Additionally, current national cyber goals include creating more in-house cyber security features, and new legislation strengthening the requirements imposed on internet service providers (ISPs) to block fraudulent and/or malicious web pages. Ongoing changes include legal and regulatory adjustments in government salaries for professionals in IT, making government employment more competitive, and increasing EU grant applications to encourage Latvian involvement in cyber resilience efforts. Latvian cyber security communications networks have also expanded as a result of the Ukrainian war. CERT.LV, for instance, has developed a strong cyber security community with officially registered members to inform the Latvian government and industry of attacks and to exchange information with Latvia and beyond. A final development in the cyber space has

been the adoption and expansion of the Latvian model of the national guard, with the aim of growing the national pool of cyber expertise available to collaborate with defence and governance units in times of crisis.[94]

Lithuania

In Lithuania, the government has been steadily deepening its cyber institution capability and its security frameworks. In 2025, the Ministry of Defence aims to establish the nation's first Cyber Defence Force to boost cyber security capacity.[95] Bolstering this capability has been an enduring challenge for the Baltic states and Ukraine. Indeed, a key takeaway for stakeholders interviewed is that Ukraine did not have enough skilled IT people when the war began. For Lithuania, like Estonia and Latvia, acknowledgment of this deficit has led it to focus on the development of civil and voluntary forces that are increasingly regarded as significant to the achievement of national defence (as well as the 'total defence' of Lithuania).

The Lithuanian government is in the process of introducing a new bill to more systematically institutionalise the volunteer defence forces (the Lithuanian Riflemen's Union (LRU)). This change will also see cyber force units embedded in the permanent force, in reserve units, and as part of the LRU. This plan denotes the adoption of 'levels of preparedness' Vilnius has developed as part of a broader defence culture, articulated in the motto 'Will to Resist'.[96] Additional planning has included expanding joint exercises between military, universities, civil society, and businesses in the cyber domain to two per year; establishing a special cyber military force of volunteers that will be incorporated in the military in a time of crisis; and creating a cyber experts community that engages across conferences, universities and community gatherings to develop trust.

For Lithuania, the challenge of developing public–private partnerships in cyber security and resilience has been slower. Challenges, for instance, include decreasing the amount of time it takes to process security clearances from six months to two, reducing exposure of critical infrastructure to private sector dependencies where services are employed instead of in-house development, and then strengthening relationships with other EU actors.[97]

Ukraine

Ukraine's cyber defence strategy has been based on partnerships with key organisations. This public–private collaboration has been key to the country's strengthened resilience against Russian cyber threats. Ukraine's long-term success will require greater structure, sustained training, and deeper integration of civilian and private sector contributions.

The following key lessons highlight the evolving landscape of cyber warfare partnership:

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

1. Strategic international engagement has enhanced national resilience

Ukraine's partnerships with multinational corporations like Microsoft and AWS and with NATO/EU programs were pivotal in mitigating the effect of Russian cyber attacks. These partnerships provided Ukraine access to advanced technologies, expertise and resources that were otherwise unavailable domestically. Meanwhile, cross-border cooperation with the Baltic states has enhanced regional security and information sharing, sometimes on a daily basis.

2. Volunteer cyber organisations have contributed to cyber resilience

The IT Army of Ukraine (alongside other initiatives) proves that volunteer civilian hacker groups can effectively execute cyber attacks and protect against Russian influence operations. In Ukraine, these groups have been modelled on efforts undertaken in Estonia, Latvia and Lithuania, where the formalisation of cyber units in paramilitary and militia bodies has contributed to national defence. While volunteer cyber units have demonstrated their capacity to contribute to cyber resilience, questions remain about how to optimise their impact and collective skill.

3. Regional and international forums have enabled access to expertise and funding

Ukraine's participation in forums like the Ukrainian Drone Defence Forum and EU Eurosatory, and Baltic state initiatives, has facilitated collaboration with foreign industries. This has led to agreements that have significantly expanded Ukraine's technological capabilities.

4. Private sector readiness and coordination are key to national response

Ukraine's ability to recover quickly from cyber attacks was tied to private sector preparedness and the systematic interaction between public and private entities. Western governments should ensure that private sector stakeholders are not only prepared for cyber threats but also integrated into national response and recovery strategies.

5. Training and upskilling have become essential for long-term resilience

Ukraine's reliance on international partnerships for training has highlighted Ukraine's domestic cyber skill gaps. We have seen Western cyber/IT organisations providing access to the latest cyber tools and systems, as well as providing cyber security expertise. In the long term, Ukraine needs to prioritise ongoing cyber training programs to build and sustain a Ukrainian skilled workforce capable of managing current and future complex cyber security threats.

6. In the Baltics, total defence models help enhance national resilience

Estonia's and Lithuania's total defence models illustrate the importance of integrating civilians into national defence frameworks. Estonia's NDL, Latvia's National Guard and Lithuania's LRU provide training, support cyber units, and build a culture of national preparedness. In Ukraine, these models have guided civilian cyber outreach efforts to include volunteer forces that can act as force multipliers during crises. These frameworks may be less ideal or practical in contexts beyond Ukraine, but a clear benefit has been to foster a culture of cyber resilience that has contributed to national defence efforts. What is interesting, further, is that all three Baltic nations have established and administered extensive cyber community communication networks between and among partner nations and private sector enterprises.

7. Digital transformation drives innovation

We have seen that that digital transformation drives innovation especially at times of crisis. The Diia app in Ukraine serves as an example because it enables digital government operations while boosting economic growth and supporting national defence requirements. Diia also highlights how technology can link citizens to government and also to the military.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ EXAMPLE OF INDUSTRY/ PARTNERSHIP SUPPORT

The Russia–Ukraine conflict underscores the transformative role of public–private partnerships in bolstering national cyber defence and resilience efforts, serving as a critical force multiplier against sophisticated cyber threats.

As soon as the conflict started, the Ukrainian government was able to work with Western corporations, most notably Microsoft, AWS and Google, to secure Ukraine's critical infrastructure and digital infrastructure. What we saw was an agile response from the Ukrainian government to the use of Western technologies. For future conflicts, such partnerships will likely redefine strategic responses, with multinational IT companies playing pivotal roles in the achievement of secure data hosting, advanced threat detection, recovery solutions, and advanced threat detection training. This model of integrated cyber defence emphasises the necessity for global cooperation to withstand the evolving landscape of cyber warfare.

The following examples of partnerships offer a basis for understanding and developing a framework of networked warfare that builds resilience and national cyber development into the national security response.

Secure IT/Cloud Provision

Perhaps the most significant partnership for Ukraine has been its relationships with major US cloud providers and service companies: AWS, Microsoft and Google. Before the Russian invasion in 2022, Ukrainian law required certain government data and select private sector data to be stored in servers physically located in Ukraine. A week before the Russian military invaded the country, Ukraine's parliament passed legislation to allow government and private sector data to be moved to the cloud.[98]

The rapid change to the Ukrainian laws set the circumstances for the government, with the aid of AWS, Microsoft, Google and Oracle, to migrate government records into the cloud. Ukraine's Deputy Prime Minister Mykhailo Fedorov labelled the action as the saviour of the government and economy.[99]

The following are examples of support from industry for Ukraine:

- **Microsoft** provided free storage capabilities for 'all Ukrainian government entities, including the military, schools, universities, and hospitals'. As of November 2023, this amounted to US$540 million of 'free services, technical support, equipment, and

grants'.[100] For example, Microsoft's Azure cloud computing platform has been deployed by KredoBank (one of the leading banks in Ukraine), and the bank has since added infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) to its suite to protect its data and business processes.[101] Microsoft's team worked with Ukrainian government personnel across 10 weeks to provide services from cyber defence to cloud migration.[102]

- **AWS** provided its Snowball service, a secure data transport solution, to enable Ukraine to transfer large amounts of data outside the country. This method bypassed the compromised Ukrainian networks while preserving data integrity. Additionally, AWS hosted a significant volume of data from various Ukrainian institutions, exceeding 10 petabytes. This included government records, medical records, and research data from 27 Ukrainian ministries and 18 Ukrainian universities. Meanwhile, AWS facilitated the rapid and secure migration of PrivatBank, Ukraine's largest private bank, to the cloud. This involved moving 270 applications and four petabytes of client data from 3,500 Ukraine-based servers to the cloud within 45 days. AWS has committed more than US$105 million in support to assist 'Ukrainians' short- and long-term needs, and recently launched ITSkills4U, a free workforce development initiative now providing 17,000 Ukrainian refugees with skills training and support services'.[103] AWS has rolled out extensive humanitarian and education resources, as well as cyber resources, to help the government.[104]

Fig 5 - AWS snowball vehicle, examples of which are deployed in Ukraine SnowMobile. (Source: Geekwire Photo / Dan Richman)

- **GigaCloud** is a Ukrainian cloud service provider offering a number of cloud services. Its primary market is the Ukrainian market, where it offers disaster recovery as a service (DRaaS) and backup as a service (BaaS) focused on Ukrainian businesses and government. It also provides free cloud infrastructure for dozens of military projects for the Ukrainian armed forces.[105]

The following are examples of non-strategic partnerships:

- **Oracle** is known to have been a consultant to the Ukrainian government on cloud infrastructure services. However, there is little open-source information available on what services, if any, it has provided. Oracle has donated over US$1 million in humanitarian aid and has matched employee contributions to charities helping Ukraine.[106] Additionally, it has ceased all operations in Russia and Belarus and has pledged not to enter into any new contract with Russian or Belarusian companies, subsidiaries or partners.[107]

- **Google Cloud** launched cloud technology training programs to support Ukrainian businesses and IT professionals. Google's support fund of almost US$10 million will finance Ukrainian start-ups. Thirty-five start-ups will receive up to US$100,000, mentoring support and Google Cloud credits.[108] In addition, Google has provided mentorship, product support and up to US$350,000 in cloud credits to the private sector.[109] As well as humanitarian aid, Google has donated 50,000 Chromebooks for use in Ukrainian schools and, until August 2023, extended free access to premium Google Workspace for Education within Ukrainian universities and colleges.[110]

Cyber Tools and Capabilities

Ukraine's ability to withstand relentless cyber attacks during the ongoing conflict has been profoundly shaped by its partnerships with global cyber security leaders. Western companies have provided essential tools, resources and expertise to help Ukraine protect its critical infrastructure against a wide range of cyber security attacks. These partnerships have been key in enabling Ukraine to overcome some of it cyber weaknesses. They have also allowed Ukraine to access leading-edge technologies. Ultimately, these partnerships have enabled Ukraine to detect and mitigate advanced cyber security threats, defend against coordinated DDoS attacks, and protect Ukraine's critical infrastructure.

Some key examples of corporate partnership include:

- **ESET**, a Slovakian company, specialises in detecting, mitigating malware. It has provided ongoing cyber security solutions to Ukraine since 2022. In addition to deploying its expert threat intelligence team to work with CERT.UA on threat detection and mitigation, it has offered free upgrades of its highest-grade solutions to critical Ukrainian institutions and extended consumer licenses at no cost.[111] The company has

also developed tools to counter specific malware threats that have targeted Ukraine, and it has collaborated with Microsoft and Ukrainian CERT.UA teams to disable targeted attacks against energy providers by the APT Sandworm hacking group.[112] Other support has included training and resilience-building efforts. It has also actively engaged the cyber security community through conferences and educational events.

- **Cloudflare** is a USA company that offers DDoS attack protection and zero trust network access. Since the invasion, Cloudflare has protected key Ukrainian websites from DDoS attacks and offered secure network infrastructure. It has supplied secure zero trust network solutions to more than 60 organisations in Ukraine and has tracked internet outages, reporting them publicly. Cloudflare also offers free services and expedited onboarding of its Project Galileo, which provides free security and mitigation efforts against DDoS attacks.[113]
- **Cisco Talos Intelligence Group** is a USA cyber security company. It set up an internal Ukraine task unit at the outset of the invasion to help with threat hunting and to monitor and detect threats against critical Ukrainian infrastructure. The team provided 24/7 critical customer care in Ukraine while, according to corporate blogs, 'over 500 employees at Cisco have joined them to assist in collecting open-source (public) intelligence'.[114] The company has extended all security licences for all Cisco customers in Ukraine. It has also provided US$1 million equivalent delivery of specially designed industrial ethernet switches to stabilise Ukraine's electricity grids amid constant electronic warfare attacks.[115]
- **Flare**, a Canada-based company, offers threat exposure management (TEM) solutions to Ukraine. Flare works closely with Ukrainian private sector firms to develop cyber infrastructure resilience. According to Flare's website, its TEM solution 'integrates cyber threat intelligence, digital risk protection, and external attack surface management to proactively manage and mitigate threats'. The initiative 'aims to support Ukraine's economic stability and resilience against cyber threats'.[116]

Threat Intelligence Services

The term 'threat intelligence services' refers to the collection, analysis and dissemination of information about potential or active cyber security threats to help organisations anticipate, prepare for and mitigate attacks. Threat intelligence services provide information about malicious actors and their methods, tools and targets, and about ways to protect against them. Threat intelligence involves a number of activities including monitoring threat activities, identifying vulnerabilities, sharing indicators of compromise (IOCs) and offering advice on how to protect against the threats.

In the Ukrainian context, Western IT organisations have been supporting the Ukrainian government and military to protect their critical systems. This support has taken the form of threat intelligence sharing and forecasting regarding APTs, offering technologies to combat ransomware.[117]

These services have also been vital in efforts to detect and mitigate attacks on critical infrastructure (including energy grids and financial systems) that has often been targeted with sophisticated malware attacks. Over the course of the war, many Western organisations have contributed to maintaining Ukraine's cyber threat resilience, and as a result these organisations have also been able to improve their technologies based on their experiences.[118] The following examples highlight some of the support provided by Western IT organisations:

- **Bitdefender**, a Romania-based cyber firm, is offering threat intelligence, technical consulting, and cyber security technology to 'Ukraine-based businesses, government bodies or private citizens for as long as they might need it'.[119] According to the company's website, it does this by providing 'cyber security technology (for free for a year) to any company or public entity from a NATO or European Union country that seeks to enhance their cyber security posture by replacing cyber security solutions that present trust concerns from a technical or geopolitical perspective'.[120]
- **Unit 42, Palo Alto Networks** is a US-based network security organisation. Unit 42 provides global threat intelligence and has been working with the State Cyber Protection Centre of the SSSCIP of Ukraine. The focus has been on sharing threat intelligence and threat trends and improving cyber resilience for the Ukrainian government and critical infrastructure.[121]
- **Akamai** is a US company focused on network security, cloud services and cyber security. It has provided specific API protection (WAAP) technology to Ukraine, helping to protect the country against malware attacks and DDoS campaigns. Akamai's WAAP solutions have been used to protect key Ukraine government websites and critical infrastructure against cyber security attacks, as well as offering botnet protection.[122]
- **Vectra AI** is a US-based company focused on cloud security, network security and AI applications. The company has offered the Ukrainian government free access to its technologies to help secure Microsoft infrastructure and AWS cloud systems, as well as providing real-time threat intelligence.[123]
- **Google (Mandiant, Google Cloud)** has consistently provided technical aid to Ukraine to help counter Russian cyber attacks. In addition to conducting compromise assessments, providing incident response services and sharing cyber threat intelligence, Google has provided security transformation services 'to help the Ukrainian government detect, mitigate, and defend against cyber attacks'.[124] Google's

Project Shield, in cooperation with Jigsaw and powered by Google Cloud Armor, also provides free unlimited protection against DDoS attacks for the Ukrainian government and the country's private sector entities.

- **Microsoft** has been supporting Ukraine by providing threat intelligence, cloud security, critical infrastructure protection and cloud infrastructure.[125] Microsoft has also been providing Ukrainians with real-time threat intelligence. Further, Microsoft has made this information public in the form of cyber security threat trends reports.[126]

Infrastructure

The most notable example of infrastructure support to the Ukraine government has been provided by Starlink. Space X's Starlink satellite system has been operational in the war since March 2022 and has played key role in protecting Ukraine.

At the beginning of the war, with Russia heavily targeting communications-critical infrastructure, Starlink provided thousands of Starlink kits, including battery power systems, to mitigate disruptions and provide secure internet connection.[127] By July 2022, 15,000 terminals were operating in Ukraine, contributing to military operations by connecting Ukraine special operations units in the field to military command centres.[128] Starlink is 'the first satellite communications firm to emplace a robust network of thousands of low-cost, low earth orbit (LEO) satellites to enable high-speed commercial broadband connectivity almost anywhere on the globe'.[129] Due to Starlink's early adoption and integration with Ukraine's military communications architecture, it has become a key service for the command and control of combat operations, including the use of UAVs and unmanned maritime surface vehicles (UMSVs).[130] While the military continues to employ Starlink systems, most Ukrainians rely on other internet providers. This is due to the lack of infrastructure connectivity in rural areas and internet disruptions closer to front lines.

The Starlink example highlights the limits of technological superiority and the means by which commercial organisations may be willing to limit capabilities. For the first few years, Starlink offered significant advantages over Russian capabilities, but investigations have revealed that Russian armed forces have now acquired Starlink systems though illicit networks and have been employing them on the front lines to good effect. Where 'connectivity has allowed leaders to guide assaults with live drone feeds, tweak artillery coordinates by viewing impacts and assess where enemies may be their most vulnerable to attack', Russian forces are now doing the same, eroding Ukraine's advantage over Russia's more modernised forces.[131] Starlink has the ability to disconnect individual terminals and geofence devices from working in certain areas, but so far there has been little information on whether the company is helping Ukraine to achieve this.
One suggestion has been for 'Kyiv and Washington to collect terminal IDs and provide them to SpaceX, with direction to deny access to anything else'.[132]

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ IMPLICATIONS FOR THE AUSTRALIAN ARMY

The war in Ukraine has underscored the critical role of public–private partnerships in achieving national cyber resilience, particularly in securing key IT and cyber value chains.

Since the 2022 Russian invasion of Ukraine, many Western organisations have withdrawn from Russia. The Western cyber and IT sector also withdrew from the Russian markets, which highlighted Russian dependency on Western IT technologies and services and introduced Russia to new cyber vulnerabilities. The situation also arose that Russian IT companies and services were banned, particularly by many Western governments, including Australia. An example is the Kaspersky Lab, including its anti-malware products and its web services.[133]

If there were a future conflict involving Australia, what would be the impact from a partnership perspective? Could Australia rely on Western IT companies to provide the required cyber services and cyber infrastructure?
From the perspective of national sovereign capabilities, would Australia, with a small cyber industry/start-up community and small defence industry base, be able to support its national defence commitments at a time of need?

A key lesson from the ongoing conflict in Ukraine is that cyber resilience is not just the role of government. It needs corporations, start-ups, small businesses, and individual citizens to work together to protect critical infrastructure. Technology companies (Western and Ukrainian) play a key role in protecting Ukraine's cyber defences by protecting critical infrastructure and spearheading ongoing cyber operations.

Western companies, from the start of the war, helped to mitigate cyber attacks against Ukraine and provided secure communications and infrastructure. They also provided cloud storage to allow for the secure storage of key data. These relationships took time; they were built on trust, transparency and common objectives. In Australia, do we have the same relationships and, at a time of need, could we rely on those companies to provide key support and services?

While government agencies such as the Australian Signals Directorate (ASD), Defence Science and Technology (DST) and Australian Cyber Security Centre (ACSC) engage with industry and research institutions, does the level of structured cooperation and support seen in Ukraine exist in Australia? It is important to strengthen these relationships to ensure that Australia's cyber resilience extends beyond government institutions into the broader digital ecosystem.

The Australian Civil-Military Centre (ACMC) provides a potential mechanism for coordinating whole-of-society responses to many types of crises. The ACMC was established in 2008 to assist Australian government agencies with overseas crisis management, including humanitarian emergencies and conflict situations. Its core mission focuses on conventional disaster management and policing within Australia and the Pacific region. In pursuit of its mission, the ACMC predominantly conducts engagement-driven exercises and workshops.

While the ACMC's responsibilities have grown in recent years to encompass wider crisis response activities,[134] its focus remains largely on traditional disaster management, policing, and regional security efforts.[135] The ACMC maintains principles for inter-agency cooperation and multi-agency coordination, but its activities and outcomes reveal a limited focus beyond the Pacific region. Further, there is little emphasis on integrating private sector partnerships in a cyber security context, particularly in public–private cooperation in securing critical infrastructure.

In view of emerging global security challenges, the role of the ACMC may need to expand. Ukraine's experience highlights the importance of including cyber and technology firms in national cyber strategies, ensuring that crisis response mechanisms are not limited to government agencies alone. Given the increasing importance of cyber security in contemporary defence planning evident in the Defence Strategic Review, the Integrated Investment Program and platforms such as AUKUS, the time may have come to change and expand the ACMC's role and focus. The capability of the ACMC to achieve multi-agency coordination is valuable, but it currently lacks focus. In theory, cyber security could be included as part of the ACMC's ongoing program of exercises. Fostering private sector partnerships in this way offers the ACMC a real opportunity to fulfil a necessary coordination function on behalf of the Australian government.

Fig 6 - Two soldiers raise the Australian flag. (Source: Adobe / Vladimir Floyd)

Given these considerations, several key recommendations emerge for the Australian Army to strengthen cyber resilience through enhanced public–private collaboration and partnership.

Recommendations

The key recommendations identified are:

1. **Development of an Australian public–private cyber partnership model**

   Australia should develop a national public–private cyber partnership model that formally integrates private sector capabilities with the those of the Australian government, including Defence. Key elements of this model include joint strategic planning, regular joint exercises, and vetting of private sector staff. A key issue for non-military organisations will be to ensure they understand how the military works in terms of methods, culture and terminology.

   The model would allow partnerships to be developed with Australian IT / cyber security organisations, Australian start-ups, and multinational IT / cyber security organisations, so that in the event of a crisis, all partners can be rapidly coordinated. The Australian Army would need to cultivate long-term relationships to ensure the success of such a model.

2. **Relationship management for multinational partnerships to balance commercial interests and strategic national security needs**

   The Australian Army should develop clear boundaries and incentives for multinational partnerships to balance commercial interests with strategic national security needs. This should also include efforts to better understand how multinational companies use technologies and services. This measure would ensure that no misunderstandings occur during a crisis. This recommendation could be supported at times of need by establishing formalised agreements for processes detailing the scope of services, performance standards and security standards that would need to be adhered to. In an ideal world, these formalised agreements would be set up before the emergency occurred. This would allow the Australian Army and the private organisations to train together, becoming familiar with the operational considerations, and wargame real-life scenarios to prepare all parties. It would also be necessary to vet multinational staff prior to any engagement to mitigate insider threats.

3. **Development of contractual frameworks to allow the use of global infrastructure when a crisis occurs**

   The Ukraine situation highlighted the importance of global infrastructure, such as the global Starlink LEO satellite system. The Australian Army should develop contractual frameworks to allow for global privately based infrastructure to be used by the Australian Army and Defence to augment existing Australian Army capabilities and infrastructure. Such frameworks should be supported by strategic partnerships that encourage corporate engagement while protecting national security interests, as well as defining any operational limitation on the use of that infrastructure.[136]

4. **Development of an Australian national cyber reserve force**

   Australia faces a key challenge: a national cyber security shortage of 30,000 professionals which impacts Australian industry, the Australian Army and the broader defence context. The Australian government should develop a national cyber reserve force that includes vetted, trained personnel who can be mobilised in times of crisis. This capability could help inform a potential Australian public–private cyber partnership model, where organisations' cyber workforces could assist the ADF at times of crisis. The ASD operates a Cyber Gap Program, but further efforts may be required to scale up a national cyber reserve.[137]

5. **Development of deep relationships with European partners**

   Australia should seek to develop partnerships with like-minded countries. Historically Australia has not partnered at scale in Europe due to geography and costs. Recently this situation has changed—for example, with the provision of Bushmaster Infantry Mobility Vehicles to Ukraine,[138] ADF training of Armed Forces of Ukraine members[139] in the UK, and the newly announced European Defence Investment Fund.[140]

   To learn from European lived experiences, there is an opportunity for Australia to become more involved in European defence and cyber initiatives within NATO and the EU. In this regard, Australia should consider becoming a member of the Regional Cyber Defence Centre (Regioninis kibernetinės gynybos centras) in Lithuania. Membership of this organisation would allow Australia to understand the cyber experience of the Baltic states and of other key European partners in the Centre, including Ukraine.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ CONCLUSION

The war in Ukraine (2020–present) has demonstrated the importance of government partnerships with private organisations. The Ukrainian experience has highlighted that security is at the core of digital transformation. Public–private cyber partnerships have been an important element in Ukraine, with Western IT companies providing cyber tools, services and intelligence, and volunteer cyber groups forming to support Ukraine. The Ukrainian government has been successful in developing these key partnerships because they have their genesis in trusted relationships that have been established over an extended period of time.

Fig 7 – Military badge of Ukrainian Army with trident and yellow-blue flag on the uniform of a Ukrainian soldier. (Source: Dmy To)

Australia can learn from the Ukrainian experience in terms of the need to develop a strong Australian public–private cyber partnership model, methods of working with international organisations, an Australian cyber reserve, and ways in which we can build stronger relationships with our European partners.

The Ukrainian experience has highlighted the importance of national agility, the ability to adapt security relationships and partnerships, and the willingness to react to emerging situations as they evolve. Australia needs to anticipate future trends and challenges in order to stay ahead of our adversaries, but it also needs to spend the time to develop its own sovereign capability, especially in the cyber security domain.

This research has taken the RMIT team to Estonia, Latvia and Lithuania and to the borders of Russia and Belarus to understand the complexity of the partnership between defence, society and private companies in the Ukrainian and Baltic context. The team has had the unique opportunity to meet with industry, government, non-government agencies and defence personnel and representatives from Australia, Estonia, Latvia, Lithuania, NATO and the Ukraine as part of this research. Ukraine and the Baltic states are facing unique cyber security and hybrid threats and national security challenges that Australian society would have no understanding of. The lived security experiences of Ukraine and the Baltic states are unique. There are many things that the Australian Army can learn from those experiences.

Australian Army Occasional Paper No. 35
Cyber Security - Partnership between Defence, Society and Private Companies - Lessons from Ukraine

/ ABOUT THE AUTHORS

Professor Matthew Warren

Professor Matthew Warren is the Director of the RMIT University Centre of Cyber Security Research and Innovation and a Professor of Cyber Security at RMIT University, Australia. He is the co-director of the Australian Lithuanian Cyber Research Network.

Professor Warren is a researcher in the areas of cyber security and information warfare. He has also attracted research funding from numerous sources, including funding from the Australian Research Council, the Australian Government (Australian Signals Directorate; Department of Education, Skills and Employment; Department of Foreign Affairs and Trade; Department of Defence; Department of Education; Department of Industry, Science and Resources; and Tertiary Education Quality and Standards Agency) and the State Government of Victorian State Government, Engineering and Physical Sciences Research Council funding from the UK, EU research funding, funding from the Science Council of Lithuania, and funding from the South African National Research Foundation. He has authored and co-authored over 300 books, book chapters, journal papers and conference papers.

In recognition of Professor Warren's contribution to cyber security he has been twice awarded the Cyber Security Researcher of the Year Award by AISA (Australian Information Security Association) and is a recipient of an ACS (Australian Computer Society) President Award for his cyber security contribution. Professor Warren is a Fellow of AISA and a Fellow of the ACS.

Dr Adam Bartley

Dr Adam Bartley is a post-doctoral fellow at RMIT University's Centre for Cyber Security Research and Innovation, where he researches the nexus between international security and the challenges of emerging technologies, with a focus on artificial intelligence, information warfare, and cyber. In this capacity, he is also the program manager of the AI Trilateral Experts Group, examining the rise of mini-lateral technology groupings in the context of the AI revolution in security affairs.

Dr Bartley has spent considerable time in the United States and China, where he has engaged in research. As a Fulbright Scholar, he undertook a research fellowship with the George Washington University's Elliott School for International Studies and he has had previous fellowships with the Pacific Forum, examining grey zone challenges in the

Indo-Pacific. In addition to this, he is the managing editor for the Australian Institute for International Affairs's *Australian Outlook*.

Professor Aiden Warren

Professor Aiden Warren is based at the School of Global, Urban and Social Studies at RMIT University in Melbourne and is Theme Leader (National Security) at the Centre for Cyber Security Research and Innovation. His teaching and research interests are in the areas of international security, US national security and foreign policy, US politics (ideas, institutions, contemporary and historical), international relations (especially great power politics), issues associated with weapons of mass destruction proliferation, non-proliferation and arms control, and emerging technologies.

Professor Warren is a Fulbright Scholar and has spent extensive time in Washington DC completing fellowships at the James Martin Center of Non-proliferation, the Arms Control Association, and the Institute for International Science and Technology Policy at George Washington University. He is the author of *US Foreign Policy and China: Security Challenges across the Bush, Obama and Trump Administrations* (Edinburgh University Press, 2021) and Understanding Presidential Doctrines (Rowman and Littlefield, 2022).

/ ENDNOTES

1 'Cyber resiliency', Glossary, NIST Cyber Security Resource Centre, *National Institute of Standards and Technology*, accessed June 3, 2025, at: https://csrc.nist.gov/glossary/term/cyber_resiliency.

2 'Ukraine Country Profile', *BBC News*, 27 January 2025, at: https://www.bbc.com/news/world-europe-18018002.

3 George Ingram and Priya Vora, 'Ukraine: Digital Resilience in a Time of War', *Brookings Institution*, 30 January 2024, at: https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/.

4 Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar', *Wired*, 28 June 2017, at: https://www.wired.com/story/russian-hackers-attack-ukraine/; Glib Pakharenko, 'Cyber Operations at Maidan: A First Hand Account', in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (NATO CCD COE Publications, 2015).

5 K Giles, *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine* (Chatham House, 2023), at: https://doi.org/10.55317/9781784135898chathamhouse.org+6chathamhouse.org+6chathamhouse.org+6.

6 J Przetacznik and S Tarpova, *Russia's War on Ukraine: Timeline of Cyber-attacks*, EPRS Briefing No. PE 733.549 (European Parliamentary Research Service, 2022), at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

7 Grace B Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C Maness and Jose M Macias. *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures* (Washington, DC: Center for Strategic and International Studies, 2023), at: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

8 Ibid.

9 Ibid.

10 Maggie Miller, 'Russian Invasion of Ukraine could Redefine Cyber Warfare', *Politico*, 28 January 2022, at: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

11 Nick Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense', *Carnegie Endowment for International Peace*, 3 November 2022, at: https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en.

12 Andy Greenberg, 'Ukraine Suffered More Data-Wiping Malware Last Year than Anywhere, Ever', *Wired*, 22 February 2023, at: https://www.wired.com/story/ukraine-russia-wiper-malware/.

13 Maria Henriquez, 'Microsoft Finds FoxBlade Malware in Ukrainian Systems', *Security Magazine*, 3 March 2022, at: https://www.securitymagazine.com/articles/97198-microsoft-finds-foxblade-malware-in-ukrainian-systems.

14 'Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future', *Amazon News*, 9 June 2022, at: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

15 'Ukrainian Digital Journey: Estonia's Role in Ukraine's EU Integration', *e-Estonia*, 13 March 2024, at: https://e-estonia.com/estonian-ukrainian-digital-cooperation/.

16 'Lithuania Delivers Final Batch of Crowdfunded Anti-Drones to Ukraine', *LRT*, 28 August 2024, at: https://www.lrt.lt/en/news-in-english/19/2348336/lithuania-delivers-final-batch-of-crowdfunded-anti-drones-to-ukraine.

17 Olga Oliker, Lynn E Davis, Keith Crane, Andrew Radin, Celeste Gventer, Susanne Sondergaard, James T Quinlivan, Stephan B Seabrook, Jacopo Bellasio, Bryan Frederick, Andriy Bega and Jakub P Hlavka, *Security Sector Reform in Ukraine* (RAND Corporation, 2016), at: https://www.rand.org/pubs/research_reports/RR1475-1.html.

18 Kotliarov, Yurii, Tsyba, Serhii, & Kurylina, Viktoriia. *Cybersecurity 2024*. Asters Law Firm, 14 March 2024, at: https://www.asterslaw.com/press_center/publications/cybersecurity_2024/

19 Samuel Charap and Scott Boston, 'U.S. Military Aid to Ukraine: A Silver Bullet', *Rand Commentary*, 21 January 2022, at: https://www.rand.org/pubs/commentary/2022/01/us-military-aid-to-ukraine-a-silver-bullet.html.

20 The White House, Office of the Press Secretary, 'Fact Sheet: U.S. Assistance to Ukraine', *The White House: President Barack Obama*, 21 November 2014, at: https://obamawhitehouse.archives.gov/the-press-office/2014/11/21/fact-sheet-us-assistance-ukraine.

21 'Ukraine Cybersecurity Assistance', *International Trade Administration*, 30 September 2020, at: https://www.trade.gov/market-intelligence/ukraine-cybersecurity-assistance.

22 Equipo Nizkor & Derechos Human Rights. *NATO's practical support to Ukraine*. Derechos.org, 5 February 2015, at: https://www.derechos.org/peace/russia/doc/ukrnato74.html

23 Ibid.

24 Ibid.

25 Ibid.

26 *National Cyber Security Strategy of Ukraine* (Kyiv: National Security and Defense Council of Ukraine, 2016), at: https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf.

27 Ibid.

28 Ibid.

29 Ibid.

30 Interfax-Ukraine, 'Poroshenko Signs Law on Key Principles of Ensuring Ukraine's Cyber Security', *Kyiv Post*, 7 November 2017, at: https://www.kyivpost.com/ukraine-politics/poroshenko-signs-law-key-principles-ensuring-ukraines-cyber-security.html.

31 Lucian Kim, 'How U.S. Military Aid Has Helped Ukraine Since 2014', *NPR*, 18 December 2019, at: https://www.npr.org/2019/12/18/788874844/how-u-s-military-aid-has-helped-ukraine-since-2014.

32 Oleh Semenenko, Uzef Dobrovolskyi, Maryna Sliusarenko, Ihor Levchenko and Serhii Mytchenko, 'Legal Aspects of the Cybertechnology Development and the Cyberweapon Use in the State Defence Sphere: Global and Ukrainian Experience', *Social & Legal Studios* 6, no. 4 (2023): 194, at: https://doi: 10.32518/sals4.2023.192.

33 Vera Zimmerman, 'Ukraine's Finally Got a Cybersecurity Strategy. But Is It Enough?', *Atlantic Council*, 20 April 2016, at: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-s-finally-got-a-cybersecurity-strategy-but-is-it-enough/.

34 Nataliya Tkachuk, 'National Cyber Security System of Ukraine: Perspectives of Policy Development and Capacity Building', *Internauka* 7 (2019): 2, at: https://doi.org/10.25313/2520-2308-2019-7-5340. See also Tom Johansmeyer, Gareth Mott and Jason RC Nurse, 'Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experiences of War', *The RUSI Journal* 169, no. 3 (2024): 48.

35 Johansmeyer, Mott and Nurse, 'Cyber Strategy in Practice', 48.

36 'The President of Ukraine Approved a New Cybersecurity Strategy of Ukraine', *National Security and Defense Council of Ukraine*, 27 August 2021, at: https://www.rnbo.gov.ua/en/Diialnist/4976.html.

37 Natalia Spînu, *Ukraine Cybersecurity: Governance Assessment* (Geneva Centre for Security Sector Governance, 2020), p. 4, at: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

38 Tkachuk, 'National Cyber Security System of Ukraine'.

39 Ibid.

40 'The Law of Ukraine: On the Introduction of Changes to Some Laws of Ukraine Regarding Urgent Measures to Strengthen Capabilities for Cyber Protection of State Information Resources and Objects of Critical Information Infrastructure', *Verkhovna Rada*, January 2023.

41 Romina Bandura, Ilya Timtchenko and Austin Hardman, 'Supporting Ukraine's Private Sector during Wartime', *Center for Strategic and International Studies*, 7 February 2024, at: https://www.csis.org/analysis/supporting-ukraines-private-sector-during-wartime.

42 'eGA to Support Ukraine's Digital Transformation with €17,4 M', *e-Estonia*, 21 February 2023, at: https://e-estonia.com/ega-to-support-ukraines-digital-transformation-with-e-174-m/.

43 Ibid.

44 Franklin D Kramer, 'The Sixth Domain: The Role of the Private Sector in Warfare', *Atlantic Council*, 4 October 2023, at: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/.

45 Ronald Bearse, '"Understanding Critical Infrastructure" from Enabling NATO's Collective Defense CISR (NATO COE-DAT Handbook 1)', Episode 10, *Conversations on Strategy Podcast*, Strategic Studies Institute, US Army War College, 6 January 2023, at: https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Article/3946047/understanding-critical-infrastructure-from-enabling-natos-collective-defense-ci.

46 SV Sieriebriak, 'Public-Private Partnership in the Field of Cybersecurity', *Analytical and Comparative Jurisprudence* 6 (2024): 22, at: https://doaj.org/article/61525fc054d440b5b16da3e130bfd827 and https://www.researchgate.net/publication/387333353_Public-private_partnership_in_the_field_of_cybersecurity.

47 Greg Rattray, Geoff Brown and Robert Taj Moore, The Cyber Defense Assistance Imperative: Lessons from Ukraine (Aspen Institute, February 2023), at: https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf.

48 Henriquez, 'Microsoft Finds FoxBlade Malware in Ukraine Systems'.

49 'Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future', *Amazon News*.

50 Andrii Paziuk, Ellina Shnurko-Tabakova, Oles Osadchyi, Andrii Davydiuk, NataliyaTkachuk, Sergii Prokopenko, Olexandr Bakalynskyi, Mykola Kuleshov, Roman Proskurovskyi and Maryna Yevdokymenko, 'A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience', *Cyber DIIA*, 11 February 2024, at: https://nsarchive.gwu.edu/document/32135-30-cyber-diia-decade-trenches-cyberwarfare

51 Ibid.

52 Ibid.

53 M Warren, D Štitilis, M Laurinaitis and S Khan, 'Hybrid Threats: The New Generation of Threats', *International Journal of Contemporary Intelligence Issues* 1, no. 2 (2024).

54 Raphael Satter, 'Satellite Outage Caused "Huge Loss in Communications" at War's Outset—Ukrainian official', *Reuters*, 16 March 2022, at: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

55 Anushka Kaushik, *The War on Ukraine: A Look at (Underemphasised) Russian Cyber Operations* (Bratislava: GLOBSEC, February 2023), at: https://www.globsec.org/sites/default/files/2023-02/cyber%20brief%20russian%20cyber%20operations-v6.pdf.

56 Ibid.

57 C Todd Lopez, 'In Cyber, Differentiating between State Actors, Criminals Is a Blur', *U.S. Department of Defense*, 14 May 2021, at: https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/.

58 Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy and Anina Schwarzenbach, National Cyber Power Index 2020: Methodology and Analytical Considerations (Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2020), p. 13, at: https://www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf.

59 ITU, *Measuring Digital Development: Facts and Figures 2019*, (ITU Publications, 2020), at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

60 Dan Jerker B Svantesson, 'Regulating a "Cyber Militia"—Some Lessons from Ukraine, and Thoughts about the Future', *Scandinavian Journal of Military Studies* 6, no. 1 (2023): 89, at: https://doi.org/10.31374/sjms.195.

61 Kotliarov, Tsyba and Kuryilna, 'Cybersecurity 2024'.

62 Joe Tidy, 'Meet the Hacker Armies on Ukraine's Cyber Front Line', *BBC*, 15 April 2023, at: https://www.bbc.com/news/technology-65250356.

63 Caroline Frost, 'Russia's State TV Hacked: Millions Told "The Hour of Reckoning Has Come"—In Ukrainian', *Yahoo*, 15 July 2023, at: https://www.yahoo.com/entertainment/russia-state-tv-hacked-millions-113800186.html.

64 Anushka Kaushik, *Ukraine's Cyber Defence: Insights on Private Sector Contributions since the Russian Invasion* (GLOBSEC, June 2023), at: https://www.globsec.org/sites/default/files/2023-06/Ukraines%20cyber%20defence%20-%20Insights%20on%20private%20sector%20contributions%20since%20the%20Russian%20invasion.pdf.

65 Tidy, 'Meet the Hacker Armies on Ukraine's Cyber Frontline'.

66 Kaushik, 'Ukraine's Cyber Defence'.

67 Daryna Antoniuk, 'Ukraine's Defense Ministry Launches Military CERT to Counter Russian Cyber Attacks', *The Record*, 9 October 2024, at: https://therecord.media/ukraine-creates-military-cert.

68 Kotliarov, Tsyba and Kuryilna, 'Cybersecurity 2024'.

69 Ibid.

70 'Estonian Defence League: Security of Statehood Initiated by the People', *Kaitseliit*, at: https://www.kaitseliit.ee/en/history-of-the-edl-cu.

71 Kateryna Bondar, 'Arsenal of Democracy: Integrating Ukraine into the West's Defense Industrial Base', *Carnegie Endowment for International Peace*, 4 December 2023, at: https://carnegieendowment.org/research/2023/12/arsenal-of-democracy-integrating-ukraine-into-the-wests-defense-industrial-base?lang=en.

72 'Arsenal of the Free World: Results of the First International Defense Industries Forum', *Ministry of Strategic Industries of Ukraine*, 30 September 2023, at: https://mspu.gov.ua/en/news/arsenal-of-the-free-world-results-of-the-first-international-defense-industries-forum.

73 'Kinstellar and Strategy Council Present the Ukrainian Drone Defence Forum London', *Kinstellar*, May 2024, at: https://www.kinstellar.com/news-and-insights/detail/2825/kinstellar-and-strategy-council-present-the-ukrainian-drone-defence-forum-in-london.

74 Oleksandra Amru, 'Air Defense Modernization, Service Center and Joint Development of Drones. Ukrainian Companies signed Seven Agreements with European Companies', *Babel*, 20 June 2024, at: https://babel.ua/en/news/108279-air-defense-modernization-service-center-and-joint-development-of-drones-ukrainian-companies-signed-seven-agreements-with-european-companies.

75 Sarah Young, 'UK Firm Supports Ukrainian Armed Forces in Drone Tech Race', *Reuters*, 28 March 2024, at: https://www.reuters.com/business/aerospace-defense/uk-firm-supports-ukrainian-armed-forces-drone-tech-race-2024-03-27/.

76 The nations include the United States, Canada, Denmark, Estonia, France, Germany, the Netherlands, Poland, Sweden and the United Kingdom. Daniel Pereira, 'The "Tallinn Mechanism" is Designed to Enhance Civilian Cyber Assistance to Ukraine', *OODA Loop*, 4 January 2024, at: https://www.oodaloop.com/archive/2024/01/04/the-tallinn-mechanism-is-designed-to-enhance-civilian-cyber-assistance-to-ukraine/.

77 'Cyber Defense Assistance Collaborative (CDAC) Case Study: Threat Intelligence Sharing', *CRDF Global*, 1 April 2024, at: https://crdfglobal-cdac.org/case-study-threat-intelligence-sharing/.

78 Gulsanna Mamediieva, 'Ukraine's Digital Transformation: Innovation for Resilience', *Harvard Center for International Development*, 1 April 2025, at: https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience.

79 Ibid.

80 'Diia: Digital State', *Kitsoft*, at: https://kitsoft.ua/projects/diia-digital-state; 'Frequently Asked Questions', *Diia*, accessed 29 January 2025, at: https://diia.gov.ua/en/faq; 'Ukrainians Can Use the Test Version of the State Statistics Service's New Portal', *EPAM*, 10 November 2023, at: https://www.epam.com/about/newsroom/in-the-news/2023/ukrainians-can-use-the-test-version-of-the-state-statistics-services-new-portal.

81 'About Diia', *Diia Expo*, accessed 5 June 2025, at: https://expo.diia.gov.ua/.

82 Mykhailo Fedorov, 'У нас дуже багато талановитих українців у цифровій сфері', *Telegram*, 26 February 2022, at: https://t.me/zedigital/1114.

83 *National Cyber Security Strategy of Ukraine*.

84 Anna Lysenko and Seva Gunitsky, 'The Invisible Front: Ukraine's IT Army and the Evolution of Cyber Resistance', *Post-Soviet Affairs* 41, no. 4 (2025): 263–288, at: https://doi.org/10.1080/1060586X.2025.2503658.

85 'Estonia Saw a Record Number of Cyber Attacks in 2022', *e-Estonia*, 27 March 2023, at: https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/.

86 Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, UK, 30 June – 1 July 2008 (Reading: Academic Publishing Limited, 2008), at: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

87 Tomas Jermalavičius and Mikk Lellsaar, *Dual-Use Research and Technology (R&T) for Estonia's National Defence, Civil Security and Public Safety: Why, What and How?* (RKK International Centre for Defence Studies, June 2013), at: https://icds.ee/wp-content/uploads/2013/ICDS%20Policy%20Paper_Dual-use%20R&T_T%20Jermalavicius%20M%20Lellsaar_June%202013.pdf.

88 Interviewer 12 remarks, 4 November 2024, Tallinn.

89 Ibid.

90 Tomas Jermalavicius, *Caught between Today and Tomorrow: Defence AI in Estonia* (Defense AI Observatory, 2024), at: https://defenseai.eu/wp-content/uploads/2023/12/daio_study2320_caught_between_today_and_tomorrow_tomas_jermalivicius.pdf.

91 Interviewer 22 remarks, 7 November 2024, Riga.

92 Ibid.

93 Workshop 3 remarks, 7 November 2024, Riga.

94 Ibid.

95 Workshop 5 remarks, 12 November 2024, Vilnius.

96 Ibid.

97 Workshop 8 remarks, 14 November 2024, Vilnius.

98 'Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future', *Amazon News*.

99 Matthew Prince, 'Steps We've Taken around Cloudflare's Services in Ukraine, Belarus, and Russia', *Project Galileo by Cloudflare*, 7 March 2022, at: https://www.cloudflare.com/galileo/.

100 Nate Ostiller, 'Minister: Microsoft to Provide Free Cloud Services to Ukraine for Another Year', *Kyiv Independent*, 29 November 2023, at: https://kyivindependent.com/minister-microsoft-to-provide-free-cloud-services-to-ukrainian-government-for-another-year/.

101 'How Technology Helped Ukraine Resist during Wartime', *Microsoft*, 20 January 2023, at: https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

102 Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War', *Microsoft*, 22 June 2022, at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

103 Frank Konkel, 'How a Push to the Cloud Helped a Ukrainian Bank Keep Faith with Customers amid War', *NextgovFCW*, 30 November 2023, at: https://www.nextgov.com/modernization/2023/11/how-push-cloud-helped-ukrainian-bank-keep-faith-customers-amid-war/392375/.

104 Larry Dignan, 'AWS' Snowmobile Data Transport Truck Highlights Why Cloud Giant Is So Damn Disruptive', *ZDNet*, 30 November 2016, at: https://www.zdnet.com/article/aws-snowmobile-data-transport-truck-highlights-why-cloud-giant-is-so-damn-disruptive/.

105 'Government Has Overtaken Business in Digitalization', *GigaCloud*, February 2, 2024, https://gigacloud.ua/en/blog/novini-kompanii/derzhava-viperedila-biznes-u-tempah-cifrovizacii-publichnij-zvit-gigacloud.

106 Oracle, *Social Impact Report: Environmental and Social Impact for a Changing World* (Oracle, 2022), p. 3, at: https://www.oracle.com/a/ocom/docs/social-impact-report-2022.pdf.

107 'Update for Russian and Belarusian Companies, Subsidiaries, and Partners', *Oracle*, accessed 31 January 2025, at: https://www.oracle.com/corporate/conflict-in-ukraine/russia/.

108 Мінцифра, '$10 млн отримають українські стартапи від Фонду підтримки Google', *Telegram*, at: https://t.me/mintsyfra/6904.

109 'Ukraine Support Fund', *Google for Startups*, at: https://startup.google.com/programs/ukraine-support-fund/.

110 'Updates on Our Support for Ukraine', *Google*, 24 February 2023, at: https://blog.google/outreach-initiatives/public-policy/updates-google-support-for-ukraine/.

111 'ESET's Ongoing Support of Ukraine', *ESET*, 17 May 2023, at https://www.eset.com/uk/about/newsroom/blog/esets-ongoing-support-of-ukraine/.

112 Kris Holt, 'Ukraine Says Russian Hackers Tried and Failed to Attach an Energy Provider', *Engadget*, 12 April 2022, at: https://www.engadget.com/ukraine-russia-hack-energy-provider-eset-microsoft-162847785.html.

113 'Cloudflare Cyber Security Protection for at-Risk Sites', *Project Galileo by Cloudflare*, at: https://www.cloudflare.com/galileo/.

114 Jonathan Munshaw, 'Fighting the Good Fight: Life Inside the Talos Ukraine Task Unit', *CISCO Talos*, 23 March 2023, at: https://blog.talosintelligence.com/fighting-the-good-fight-life-inside-the-talos-ukraine-task-unit/.

115 Joe Marshall, 'Project PowerUp—Helping to Keep the Lights on in Ukraine in the Face of Electronic Warfare', *CISCO Talos*, 4 December 2023, at: https://blog.talosintelligence.com/project-powerup-ukraine-grid/.

116 'Supporting Private Sector Resilience in Ukraine through Cyber Threat Management', *Flare*, 23 January 2025, at: https://try.flare.io/chemonics-flare-collaboration/.

117 'Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities', *CrowdStrike*, 1 March 2022, at: https://www.crowdstrike.com/en-us/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/.

118 CRDF Global, 'CRDF Global Becomes Platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine', *PR Newswire*, 14 November 2022, at: https://www.prnewswire.com/news-releases/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-301676373.html.

119 Alex Scoxton, 'Cyber Companies Step up Support for Ukraine', *Computer Weekly*, 2 March 2022, at: https://www.computerweekly.com/news/252514063/Cyber-companies-step-up-support-for-Ukraine.

120 'Bitdefender & Romanian National Cyber Security Directorate (DNSC) Work Together in Support of Ukraine Bitdefender', *Bitdefender*, 23 January 2025, at: https://www.bitdefender.com/en-us/ukraine/.

121 'Unit 42 Collaborative Research with Ukraine's Cyber Agency to Uncover Smoke Loader Backdoor', *Unit 42*, 19 March 2024, at: https://unit42.paloaltonetworks.com/unit-42-scpc-ssscip-uncover-smoke-loader-phishing/.

122 'Key Ukraine Government Organizations Choose Akamai', *Akamai*, 25 October 2024, https://www.akamai.com/newsroom/customer-announcements/key-ukraine-government-organizations-choose-akamai.

123 'As the War in Ukraine Spirals, Vectra AI Announces Free Cybersecurity Services', *Vectra*, 28 February 2022, at: https://www.vectra.ai/about/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services.

124 'Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape', *Google*, 16 February 2023, at: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

125 Brad Smith, 'Extending Our Vital Technology Support for Ukraine', *Microsoft*, 3 November 2022, at: https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

126 Brad Smith, 'Defending Ukraine'.

127 Walter Isaacson, '"How Am I in This War?": The Untold Story of Elon Musk's Support for Ukraine', *The Washington Post*, 7 September 2023, at: https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/.

128 Ibid.

129 Wes J Bryant, 'When a CEO Plays President: Musk, Starlink, and the War in Ukraine', *Irregular Warfare*, 17 October 2023, at: https://irregularwarfare.org/articles/when-a-ceo-plays-president-musk-starlink-and-the-war-in-ukraine/.

130 Ibid.

131 Alex Horton, Serhii Korolchuk and Eva Dou, 'Russia's Illicit Starlink Terminals Help Power Its Advance in Ukraine', *The Washington Post*, 12 October 2024, at: www.washingtonpost.com/world/2024/10/12/starlink-russia-ukraine-elon-musk/.

132 Ibid.

133 Australian Government Department of Home Affairs, 'PSPF Direction Update—Kaspersky Lab, Inc. Products and Web Services', *Protective Security Policy Framework*, 21 February 2025, at: https://www.protectivesecurity.gov.au/news/pspf-direction-update-kaspersky-lab-inc-products-and-web-services.

134 The full statement reads: 'To strengthen Australian and regional civil-military-policy capacity and capability to respond more effectively to crises and contingencies'. ACMC home page, accessed 21 January 2025, at: https://www.acmc.gov.au/.

135 'Strengthening Civil-Military Coordination for Future Public Health Emergencies', *Defence*, 26 September 2024, at: https://www.defence.gov.au/news-events/releases/2024-09-26/strengthening-civil-military-coordination-future-public-health-emergencies.

136 Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense'.

137 '2023 ADF Cyber Gap Program Applications Now Open', *Defence*, 1 September 2022, at: https://www.defence.gov.au/news-events/releases/2022-09-01/2023-adf-cyber-gap-program-applications-now-open.

138 'Additional Support for Ukraine', *Defence Ministers*, 27 October 2022, at: https://www.minister.defence.gov.au/media-releases/2022-10-27/additional-support-ukraine.

139 Cody Tsaousis, 'Operation Marked by Mutual Respect, *Defence*, 26 November 2024, at: https://www.defence.gov.au/news-events/news/2024-11-26/operation-marked-mutual-respect.

140 'EDF: Developing Tomorrow's Defence Capabilities', *European Commission: Defence Industry and Space*, accessed 5 June 2025, at https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en.

RESEARCHCENTRE.ARMY.GOV.AU

CG: FEB 001-26