Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Private-public initiatives for cybersecurity: the case of Ukraine

Louise Axon, Jamie Saunders, Patricia Esteve-González, Julia Carver, William Dutton, Michael Goldsmith & Sadie Creese

To cite this article: Louise Axon, Jamie Saunders, Patricia Esteve-González, Julia Carver, William Dutton, Michael Goldsmith & Sadie Creese (2024) Private-public initiatives for cybersecurity: the case of Ukraine, Journal of Cyber Policy, 9:3, 399-422, DOI: 10.1080/23738871.2025.2451256

To link to this article: https://doi.org/10.1080/23738871.2025.2451256

Published online: 05 Feb 2025.

JOURNAL OF CYBER POLICY
2024, VOL. 9, NO. 3, 399–422
https://doi.org/10.1080/23738871.2025.2451256

Routledge
Taylor & Francis Group

Private-public initiatives for cybersecurity: the case of Ukraine

Louise Axon, Jamie Saunders, Patricia Esteve-González, Julia Carver, William Dutton, Michael Goldsmith and Sadie Creese

Global Cyber Security Capacity Centre, University of Oxford, Oxford, UK

ABSTRACT

Despite widespread fears at the time, Ukraine appears to have been effective in countering Russian cyber aggression since the invasion of February 2022. During the period, Ukraine has been provided with significant levels of cyber defence support by allied governments and private sector companies. Through expert interviews and roundtables, we have convened a dialogue with stakeholders with direct experience of these private-public collaborations. Our research seeks to identify the factors that have led to positive outcomes for Ukraine and the challenges experienced. We gather the insights and lessons learned for cybersecurity capacity-building and international assistance coordination and explore the applicability of such lessons to potential future crisis scenarios. This paper presents the results and makes recommendations for further work. We anticipate that the insights presented will contribute to the identification of policy and practice priorities for cybersecurity capacity-building and capability enhancements, specifically where private-public cooperation is essential to maintaining cyber resilience in the face of heightened cyberattacks. It is hoped that these insights will help states and the private sector to prepare to counter cyber aggression in other parts of the world, as well as to help sustain the continued efforts in Ukraine.

ARTICLE HISTORY
Received 15 April 2024
Revised 24 September 2024
Accepted 1 November 2024

KEYWORDS
Cyber-defence; public-private partnership; cybersecurity capacity building

1. Introduction

Cyber operations were projected by some analysts to significantly alter the initial phases of Russia's war against Ukraine, as Russia is widely considered to be a capable and willing cyber actor. The 2020 National Power Index, for example, assessed that Russia was the fourth most comprehensive cyber power across multiple domains, and third in the offensive domain, ranked only behind the US and UK (Voo et al. 2020). In the months leading up to the war, US officials expressed concerns about the potential significance of Russian 'information operations, cyber and destabilization activities' against Ukraine (Matishak 2021). However, despite evidence of a significant increase in cyberattacks against Ukraine following the invasion of 24 February 2022,[1] the operational impact of

CONTACT Louise Axon louise.axon@cs.ox.ac.uk

Russian cyber activity in the immediate aftermath of the invasion appeared much more limited than many cybersecurity experts would have predicted (Beecroft 2022; Kostyuk and Gartzke 2022; Rid 2022).

The European Cyber Conflict Research Initiative (ECCRI) found in its expert roundtable held in May 2022, approximately three months after the beginning of the conflict, that 'Russian cyber operations ha[d] been relatively unsophisticated, sometimes reworking known malware, with consequently high visibility' (Kaminska, Shires, and Smeets 2022). Further, Ukrainian sources reported in August 2023 that no critical information had been lost nor major systems taken down since the beginning of the conflict (Sorokin 2023). The reasons for this limited impact are not clear. Some experts have attributed it to the strength of Ukraine's cyber defence (Kallas 2023). Others have concluded that Russia may have taken an active decision not to deploy its most potent cyber capabilities at the start of the conflict (Sanger 2022), that it chose to focus more effort on covert activity and information influence than on disruption (Rid 2022), or that it lacked preparation (Kostyuk and Gartzke 2022). It is also important to note that many questions remain unresolved in the ongoing policy and academic debate on the relevance of cyber capabilities for shaping conflict outcomes in general (Healey 2022; Rid 2012).

Despite uncertainty about Russian intent, it is reasonable to conclude that Ukrainian cyber defences were effective in countering the increased Russian attacks that were received in the initial phases of the war. The relative decrease in major cyber disruption in the period since those initial phases suggests that Ukraine has continued to match what Russia has been able (or has chosen) to deploy against it. According to Major Yurii Myronenko, head of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), in 2022, there were 2,194 'cyber incidents' of which 1,048 were 'major or critical' (The Economist 2024). By contrast, in 2023, 2,554 incidents occurred, with only 367 characterised as serious. This paper examines the factors that have led to this apparent success, and the implications for the ongoing conflict in Ukraine and for potential cyber conflict elsewhere in the world.

Public-private partnerships (PPPs) have been widely regarded as necessary cooperation for addressing societal cyber (in)securities (Dunn Cavelty 2015), including for the purposes of cyber defence (Haklai 2023). In the context of Russia's invasion of Ukraine in 2022, this paper focusses specifically on the role of the private sector in providing assistance in the lead up to and during the war. The active role of the (Western) private sector in helping Ukrainian cyber defences has been strikingly clear, with significant levels of private sector expertise being deployed to support the protection of critical assets, and to enhance internal Ukrainian cybersecurity capability through the provision of training, specialist technology and threat intelligence. This paper examines the factors that have enabled Ukraine to absorb this assistance, and the extent to which the capabilities and relationships developed as a result of pre-war capacity-building activities have contributed to this.

Studying collaboration between public and private organisations can offer lessons that are relevant both to how assistance to Ukraine can be sustained, and to how other potential beneficiary states, allied governments and private sector partners can collaborate to counter cyber aggression in other parts of the world – noting the challenges of building capacity and enhancing capabilities quickly, using suppliers or partnerships that may be from new organisations and different jurisdictions.

Our research identifies factors that have led to positive outcomes for Ukraine, the challenges experienced, and identifies insights and lessons learned for cybersecurity capacity-building and international-assistance coordination. We explore the applicability of such lessons to potential future scenarios. Specifically, we focus on the following questions:

- What needs to be done to ensure that current capacity and capability-building efforts in Ukraine can be sustained?
- How might capacity-building activities in other countries be informed by the case of Ukraine, specifically to ensure that they are well positioned to both defend themselves and absorb crisis assistance in the event of a future nation state cyber conflict?
- What mechanisms does the international community need to establish in order to facilitate cyber defence assistance in potential future cyber conflict situations?

2. Literature review

2.1 The cyber elements of the conflict in Ukraine

The strategic impact of Russian cyber operations and their possibility of serving as an alternative to a conventional ground invasion – or as a precursor to it – has been richly debated by scholarship and policymakers. Particularly, cyber operations were projected by some analysts to significantly alter the initial phases of the regime's war against Ukraine (Kostyuk and Gartzke 2022), as Russia is widely considered to be a capable and willing cyber actor.[2]

As one senior official in the American government commented in December 2021, the Russian government has historically relied upon 'information operations, cyber and destabilization activities inside Ukraine' as part of its strategic 'playbook' (Matishak 2021). Prior to the 2022 invasion, the Putin regime hit Ukrainian critical infrastructure with cyberattacks in 2015 and targeted energy companies, government services and banks in 2017 (The Economist 2024). By 2020, the Ukrainian state security service, SBU, declared it confronts 'almost daily hacker attacks' and it had accused Russia of conducting a 'hybrid war' against the country (Reuters 2020). Indeed, 'cyber' operations have been considered by some Western commentators as part of Russia's 'hybrid warfare' approach for almost a decade (Libiseller 2023). Notably, however, the Russian doctrine uses the concept of 'information confrontation', a more encompassing concept which transcends the cyber and digital environment to include a cognitive dimension (Giles 2023).[3]

While the strategic impact of cyber capabilities remains a subject of wide academic debate,[4] one anticipated outcome of Russian cyber operations centred around the element of strategic 'surprise' (Healey 2022). For example, such a 'surprise attack' was theorised to manifest as a 'bolt from the blue' against Ukraine which would paralyse Ukrainian military forces as the precursor for Russia's ground invasion. Under such tense geopolitical conditions, cyber capabilities may induce, for example, a *fait accompli* for Ukrainian forces, thereby passing the 'burden of escalation' to American policymakers, 'who would have to choose war over political compromise'. It is worth noting that, in June 2021, the American government met with Putin to discuss a list of 'off limits' critical infrastructure in Ukraine, whereby President Biden declared publicly that if Russian-based cybercriminals struck any of the targets on the list, the US would respond (Matishak 2021). Overall, speculations about a cyber 'bolt from the blue' were often connected to fears about a 'Cyber Pearl

Harbour' – that is, a surprising and strategically significant cyberattack – against Ukraine (Healey 2022). However, this concern never materialised at the outset of the 2022 invasion. Some observers have therefore contended that cyberthreats were the 'dog that never barked' in Ukraine, having weak effects on the conflict (Kostyuk and Gartzke 2022).

Despite the absence of a 'Cyber Pearl Harbour' in the 2022 invasion, cyber conflict has nevertheless 'played out in the shadows' (Rid 2022). On 15 and 16 February 2022, Ukrainian banks were barraged by major denial-of-service (DoD) attacks, which were attributed to the Russia's intelligence service. On the one hand, the conflict has also been characterised by lower-grade DoD attacks. As such, Google announced that it would help protect over 150 websites in Ukraine from DoD attacks (Walker 2022). However, it has also featured significant attacks against Ukrainian critical infrastructure. In 2022, Mandiant, Google's threat intelligence arm, identified the Russian cyberattack 'Sandworm' against Ukrainian critical infrastructure as the 'latest evolution in Russia's cyber physical attack capability', cited as representing a 'growing maturity of Russia's offensive technology (OT) arsenal' (Mandiant 2023).

Therefore, while our case study focuses on the threat of cyberattack, it is important to acknowledge that there are other dimensions to the cyber conflict in Ukraine, such as long-term influence operations, including those in and through cyberspace, and cyberespionage (Cattler and Black 2022). In particular, there continues to be an intense conflict within the cognitive domain, with both sides seeking to shape the narrative within their respective jurisdictions and more generally across the world (Giles 2022). This potentially could influence the outcomes of cyberattacks by shaping the will of combatants and their allies to continue to fight the broader war. Cyber plays a key role in this aspect of the crisis, and it is likely that this would also be the case in other future crisis scenarios.

2.2 Public-Private partnerships in cybersecurity

Public-private partnerships (PPPs) have become central to cybersecurity, particularly as the increasing reliance on private sector infrastructure and expertise reshapes state capabilities in securing digital assets. The concept of PPPs in cybersecurity has been explored from multiple angles, ranging from incentive structures and trust-building to the evolving roles of private companies in providing cybersecurity (Collier 2018; Liebetrau and Christensen 2021; McCarthy 2018). Several scholars have noted how the dynamics of PPPs differ in cybersecurity when compared to traditional domains, often due to the critical role of private actors in maintaining national and international cyber resilience (Dunn Cavelty 2015; Haklai 2023).

One of the primary challenges in conceptualising cybersecurity PPPs lies in distinguishing between internal/domestic PPPs and those involving external assistance. Incentive structures, particularly in terms of trust, can differ significantly between these types. For example, cloud providers have emerged as dominant players in cybersecurity, reshaping PPPs by controlling significant portions of global digital infrastructure (Haklai 2023; Liebetrau and Monsees 2023). Cloud providers' global reach and monopolistic tendencies have led to debates over their roles in PPPs, especially in terms of security responsibility and data sovereignty (Lehdonvirta 2022). The dominance of cloud providers also introduces new complexities regarding trust, as states must rely on private companies that

operate across multiple jurisdictions, leading to potential conflicts in regulatory approaches and national security considerations (Haklai 2023).

Furthermore, the type of private actors involved in cybersecurity PPPs also shapes their structure and outcomes. A distinction can be made between consumer-facing technology companies and private security firms, each of which plays distinct roles in addressing cybersecurity threats. This distinction is crucial, as public consumer companies, driven by market incentives, often prioritise user acquisition and product dominance over security (Dunn Cavelty 2015). In contrast, private security firms focus explicitly on enhancing cybersecurity capabilities, often aligning more closely with governmental security objectives.

In terms of the functions that PPP can have for cybersecurity, Dunn Cavelty (2015) highlights the core function of PPPs as being for information-sharing. Haklai (2023) elaborates six expected areas of cybersecurity PPP collaboration as being information sharing; cyber defence and incident response; cyberattacks attribution; cybersecurity research and development; cybersecurity workforce development; and cybersecurity standards and best practice. Challenges are also theorised, including the difficulty of aligning priorities and incentives between the public and private sectors, liability, and the definition of clear roles and responsibilities in such partnerships. Thomas Rid describes the particular effectiveness of public-private partnership in countering adversarial intelligence operations, noting the unique advantage of the US in this regard through its 'vibrant tech and cybersecurity industry' (Rid 2022).

Pertinent to this study, scholars have explored the specific relevance of PPPs in the context of cyber aggression, including the context of the 2022 Russian invasion of Ukraine. States such as the US have increasingly recognised the strategic importance of involving the private sector in addressing cyberthreats. For Washington, PPPs have played a long-standing role in critical infrastructure protection, as reflected in the US President's *Commission on Critical Infrastructure Protection* (1997) and more recent statements by the Biden administration, as exemplified by the recently published *United States International Cyberspace & Digital Policy Strategy* (2024) and its partnership with SpaceX in the context of Ukraine (USAID 2022). However, PPPs also play an important role in the governance of cyber insecurities in the European Union context, at both the national (Christensen and Lund 2017), and supranational levels (Carrapico and Ferrand 2020; ENISA 2024; Pestarino 2023).

In summary, the literature highlights the critical role of the private sector in shaping modern cybersecurity strategies, with increasing reliance on private actors raising questions about trust, responsibility, and the boundaries of state control in ensuring national cyber resilience. The unique nature of cyberthreats, combined with the dominance of key private actors, suggests that cybersecurity PPPs require distinct frameworks compared to more traditional forms of public-private cooperation.

2.3 National cybersecurity capacity-building

National cybersecurity capacity-building has emerged as a critical area of focus for both policymakers and scholars as states seek to develop resilience against evolving cyberthreats. The academic literature on this topic centres around how nations can systematically enhance their cybersecurity posture through structured capacity-building efforts, often guided by models for assessing cybersecurity maturity.

One of the foundational aspects of cybersecurity capacity-building is the recognition that cybersecurity is not solely a technological challenge but also a governance, legal, and human issue. Scholars have emphasised the importance of a holistic approach to cybersecurity, which includes not only technical capabilities but also social, legal and policy frameworks (Dunn Cavelty 2022). This is reflected in the development of various capacity-building frameworks that incorporate multi-stakeholder engagement, legal and regulatory reforms, and public awareness campaigns. National efforts to build cybersecurity capacity thus require cross-sectoral cooperation, typically involving government agencies, the private sector, civil society and international organisations.

Models for assessing national cybersecurity capacity maturity have been developed to guide these efforts and provide benchmarks for measuring progress. One of the most widely referenced frameworks is the Cybersecurity Capacity Maturity Model for Nations (CMM), developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. The CMM evaluates five dimensions of cybersecurity capacity: policy and strategy; culture and society; education and training; legal and regulatory frameworks; and technological infrastructure. Each dimension is assessed across multiple maturity stages, from basic awareness to advanced strategic coordination, offering a comprehensive view of a nation's cybersecurity readiness (GCSCC 2021).

Other models, such as the ITU's Global Cybersecurity Index (GCI) (ITU 2024), the Potomac Institute's Cyber Readiness Index (Hathaway et al. 2015) and the Harvard Kennedy School's National Cyber Power Index (Voo et al. 2020), provide complementary approaches. The GCI, for instance, focuses on five pillars – legal measures, technical measures, organisational measures, capacity-building, and cooperation – evaluating countries' cybersecurity efforts on a global scale. The CAT, meanwhile, emphasises the economic impact of cyber risks and the integration of cybersecurity into broader national development strategies. The International Institute for Strategic Studies (IISS) developed a methodology for assessing cyber power, based on strategy and doctrine; governance, command and control; core cyber-intelligence capability; cyber empowerment and dependence; cybersecurity and resilience; global leadership in cyberspace affairs; and offensive cyber capability (IISS 2021).

In summary, the academic literature on national cybersecurity capacity-building highlights the importance of multi-dimensional approaches and structured assessments. Models such as the CMM and GCI offer practical tools for nations to evaluate and improve their cybersecurity maturity, ensuring that capacity-building efforts are comprehensive and aligned with global best practices. To inform this body of CCB knowledge, we seek to identify insights and lessons learned for cybersecurity capacity-building and international assistance coordination in this case study – in particular, providing insights on the role of cybersecurity capacities in preparing for assistance in the case of cyber conflict. The paper also provides insights on the success factors and challenges of private-public partnership in this context.

3. Research method

This case study was conducted through a dialogue involving representatives of private companies, policymakers and members of think tanks who are engaged in research or possess first-hand experience of the private sector's support for cyber resilience in

Ukraine. This particular case study was chosen as perhaps the most striking example of private-public cooperation to provide cybersecurity assistance in the context of a major conflict. Further, it is significant due to the cooperation of big technology companies and state governments. We therefore perceived value in conducting a single case study on this significant case. Case studies are a key method for research on policy and practice, particularly in areas that are new or not well developed. They enable discovery of patterns and themes that enhance understanding of otherwise less coherent or disconnected events and actions. Our approach drew on well-developed methods for case study research (Diesing 2008; Yin 2017).

We used a combination of semi-structured individual interviews with 10 experts, and two group roundtable discussions. In total, 12 experts have so far been involved in the dialogue, between May and June 2023. Our primary data therefore represents views from the initial period following the invasion. To contextualise this data, in this paper's analysis we engage with literature published since.

Interviews lasted approximately 30 min and were carried out online using video conferencing. Roundtables lasted approximately three hours and were hybrid, with some participants attending in person and some online. Participants were informed that all meetings were held under Chatham House Rule, meaning that participants may use the information from the discussions without attribution to its source.

The inclusion criteria for recruitment consisted of: (a) private companies involved in providing cyber assistance to Ukraine since the February 2022 invasion; (b) government entities involved in providing assistance; and (c) representatives from think tanks studying the provision of cyber assistance to Ukraine. The participants were recruited via emails to the contacts of the research team, or by making contact on networking platforms such as LinkedIn. The sensitivity of the topic prevents the authors from disclosing detailed demographics of the interviewees.

The questions that guided the semi-structured interviews were as follows:

- How have capacities of Ukraine been bolstered by help from the private sector?
- What are the key examples of the private-public collaborations in this space?
- What capabilities were needed? What are the key private initiatives being undertaken to address them?
- What were the processes that needed to be put in place to help bolster capacity?
- What went well in terms of the private-public collaboration, and what was challenging in terms of putting the collaboration in place?
- Are there lessons to be learnt for future situations?
- Are there capabilities that ought to benefit permanently from the lessons learnt?
- Does the experience in supporting Ukraine suggest deficiencies in cybersecurity capacities that need to be addressed in many countries?
- What are the most pertinent points in terms of learning lessons that might help other states prepare for the future?

The roundtables were run as open discussions with the group of participants, moderated by the research team. The topics addressed were: (a) which cybersecurity capacities have supported effective assistance to Ukraine in this case; (b) which cybersecurity capacities have been developed as a result of the assistance given during this conflict; (c) which

cybersecurity capacities remain lacking to support cyber defence assistance to Ukraine; and (d) what lessons can be learned from the Ukraine case study that are applicable to other potential situations requiring immediate cyber defence assistance to a nation.

Detailed written notes were captured by the researchers during the interviews and roundtables. Interpretive qualitative coding was conducted on these notes by two researchers independently, to draw out the core themes from the qualitative sources. Codebooks were developed in Word documents. The core themes were then consolidated through discussion, resulting in the final thematic coding. Interpretive coding was chosen as the analysis method to suit the exploratory and inductive nature of this research, allowing the researchers to draw out observations based on the evidence gathered (Bevir and Rhodes 2016; Thorne 2020).

3.1 Challenges and limitations of the case study

The case study is anchored in an academic institution and done in a transparent and open manner, independent of commercial or governmental influence on the conduct and findings. That said, given the political, commercial and international stakes in the conflict and its outcomes, the project faces potential barriers to the conduct of the case, and how we might mitigate them. Two prominent concerns were: access and classification. Access to participants in these cases and relevant documents are a key issue in all case study research. In cybersecurity, much of the operational work on the ground may be classified and not visible to us. There is a risk that our partial view will lead us to conclusions that are off the mark. Here we relied on rigorous approaches to the choice of interviewees and discussants and constant peer and outside reviews of working papers to avoid spurious conclusions.

It is important to note that our dialogue to date has involved only entities from the assisting community, and no representatives from Ukraine. Our interim findings are therefore based on a partial view, which is a clear limitation. Over time, we will seek to incorporate Ukrainian representation, while remaining sensitive to the necessary priorities on the Ukrainian side. Further research such as extending interviews would be valuable in order to maintain an up-to-date understanding of the issues as they evolve, and to test and identify potential implementation approaches for the recommendations for action.

4. Analysis and observations

4.1 Why private-public collaborations were needed for Ukraine

It is important to note that (in the authors' opinions), given the transnational nature of cyberattacks and their potential spillover risks, it is likely that any country would require external assistance in the case of national-scale cyberattack by a sophisticated aggressor. Further, the scarcity of skilled professionals that can defend a nation from cyberattack is not unique to Ukraine but is broadly the case worldwide. However, external assistance relationships are not only influenced by networked vulnerabilities and skills gaps, but existing political and economic relationships, including security alliances.

In the case of Ukraine, our research suggests that it was perceived (by the international community) that Ukraine's cyber defence capacity might not have matched the

cyberattacks it received from its aggressor, since Russia was assumed to be a highly sophisticated actor in cyberspace with significantly greater resources (Kello 2017; Voo et al. 2020). Whilst the ground had, to some extent, been prepared through previous years of experience of cyber aggression and associated cybersecurity capacity-building efforts, the Ukrainian cybersecurity workforce was considered to be not sufficiently orientated to counter the cyber-offensive attacks in conflict. There was, therefore, a view that there existed an immediate need to provide cyber defence assistance to Ukraine.

The private sector was motivated to play a key role in providing support to Ukraine (Liebetrau and Monsees 2023). As is discussed in greater detail later in this paper, the extent of the responsibility that needed to be taken on by the private-sector may have been increased by capacity constraints within allied governments. In our dialogue, it was suggested that public sectors generally do not have the level of agility, resources or capabilities in-house to deliver immediate practical cyber defence support on a large scale. Participants in our dialogue also shared a view that preparation and resources to provide cyber defence assistance, and in particular for partnering with the private sector to do so, may not have been prioritised sufficiently by some assisting governments to meet the initial need.

In contrast, the private sector was able to respond rapidly with agility and large amounts of resources, donating cybersecurity technologies, licences and experts. The assistance can be categorised as follows:

- Dropping in a 'shield' to actively defend specific critical assets and infrastructure, enhancing capabilities to predict, protect against, detect and respond to specific targeted aggression.
- Wide-area defence of networks at national scale – hardening internet domains and telecoms networks against DDoS and other attacks.
- Increasing the human capacity that Ukraine already had, by providing remote cybersecurity experts and network-defence operations through cloud services, and by contributing to training.
- Enhancing the intelligence picture through threat hunting and forensic analysis, and by providing access to cyber threat intelligence services.
- Migration of assets to the cloud, removing them from the battlefield and thereby reducing harm potential.

We might consider this kind of multi-sector assistance collaboration to be an example of emerging private-public partnerships;[5] different in nature to the traditional public-private partnerships, since the latter exist in the context of large-scale frameworks and can require lengthy procurement processes to establish.

4.2 Key factors for success

In Ukraine, a foundation of relationships and capacities (in particular, cyber defence skills) had been built through the ongoing experience of cyber aggression in the last decade. See, for example, the European Parliamentary Research Service's timeline of cyberattacks against Ukraine (Przetacznik and Tarpova 2022). This experience, as well as increased cybersecurity capacity-building efforts, had led to the bolstering of Ukraine's own

defensive capabilities and national cybersecurity capacity. This foundation meant that Ukraine was in a stronger position to defend itself following the invasion than it might otherwise have been, and also allowed the immediate capability enhancements provided by the international community to be effective and sustained to an extent. Furthermore, some external private sector organisations had already been working in Ukraine, in order to assist with, and learn from, the ongoing cyber aggression. This meant that companies already had trusted relationships in the country and familiarity with the infrastructure and the threat landscape, which were critical to delivering efficient and effective assistance.

The speed and force of the international response was driven in part by the mutual outrage of governments and private-sector entities in a range of countries, which led to a strong collective commitment to support. There were also perceived benefits to the private sector that drove engagement. Key benefits noted during the dialogue were: the opportunity to enhance threat knowledge (information which can in turn help to protect clients globally)[6]; the opportunity to demonstrate the benefits of technologies, in particular cloud services; increased capacity to defend in the future through practice; and the political value of being perceived to be involved for key international relationships and markets. The will and incentives of the private sector to assist aligned with the Ukrainian government's cause. This opened up resources and meant that international support was delivered quickly and robustly, to the extent that the threat could largely be countered.[7]

Also important to operational successes so far has been the ability of the collective-assistance community to act quickly and with agility. This ability has been underpinned by trusted relationships. To some extent, the private sector has been willing to act in a diffuse manner, without the usual requirements for up-front contracts, and with limited coordination. Correspondingly, the public sector in certain donor states has sought to develop approaches to partnering with the private sector that do not hinder this agility. This has been enabled by donor governments having trusted relationships with private-sector organisations that have been willing to help. Mutual understanding of working processes (e.g. due to public-private transfer of staff) has been crucial to the trust necessary to initiate projects without protracted administration.

4.3 The challenges in bolstering capacity and capability at speed

For the community delivering assistance, challenges have been posed by a lack of coordination of efforts or scoping of prioritised needs for assistance. This led, in some cases, to donors providing tools that were not used or were incompatible, or to duplication of efforts. A lack of situational awareness on the ground, or prioritisation of needs from the Ukrainian side, meant that it was not always clear what capabilities and technologies were already in place, what assistance was most urgently needed, and which types of technology would be best received by Ukraine.

There are barriers to adopting certain types of technology, apportioned to: concerns surrounding ability to maintain operational capability; resources required to learn how to effectively use new technologies and processes; reluctance to develop dependencies on service-orientated solutions because they might create ongoing requirements for continuous investment outside existing local supply-chain offerings. A key example from the Ukrainian case is legislation – which needed to be amended early in the conflict – that

prohibited the transfer of national assets to third-party cloud providers; there is reportedly continued Ukrainian concern around this.

The lack of coordination of roles and responsibilities for the various international public – and private-sector entities involved has been another key challenge. Mechanisms that were needed to support coordination were also lacking: in particular, many governments did not have mechanisms in place that would allow them to rapidly contract the private sector to provide immediate assistance following the invasion. This was compounded where private-sector companies also did not have the ability to rapidly execute contracts. Public sector representatives described the challenging trade-off between rapidly setting up contracts with room for adaptation and agility, and ensuring value for money and transparency by selecting suppliers through competition.

Furthermore, the potential liability risks to private sector responders from being involved in supporting during a conflict were not always sufficiently clearly identified or managed through legal protections.[8] Government representatives in our dialogue described challenges faced in past cases of attempting to engage with host governments to create broad memorandums of understanding (MOUs) protecting the suppliers they hire. It was noted that this is not always feasible and private-sector companies often need to set up these arrangements with the host government individually (e.g. giving permission to work on government systems and a waiver against legal action).

Some coherence has developed over time in some assisting countries: there have been ongoing conversations on the coordination of assistance, and some public-private procurement mechanisms have since been established. Challenges remain to be addressed. In developing the coordination approach, and the underlying procurement and legal mechanisms, it will be important to ensure that advantageous elements of the agile approach thus far are retained.

For Ukraine, while the presence of foundational internal cybersecurity capacities were critical to supporting its own defence and its ability to absorb assistance, there are nonetheless observable cybersecurity-capacity (and associated capability) shortfalls that have hampered the absorption of assistance.

A particular issue highlighted in the dialogue was the shortfall in sufficient numbers of skilled personnel, established roles and responsibility, coordination mechanisms, and resources (in Ukraine), to implement donated technologies, to prioritise requests for assistance, or to deliver national-scale cyber defence. While some trained experts were in place, there was also a need to pivot expertise quickly. Many professionals with technical experience as white-hat hackers or penetration testers, for example, were required to support computer network defence (threat hunting in a live system; intrusion monitoring; control orchestration): a related but different set of skills, particularly in the context of national defence. It was also highlighted that a lack of awareness of current national security posture, and importantly digital infrastructure and security tools, led to challenges in prioritising requests for assistance.

All of these issues are, of course, not unique to Ukraine. The importance of people and process, alongside technologies, as components of cyber resilience is already well understood. It has, however, been thrown into sharp relief by the challenges documented above, which were exacerbated by wartime attrition, as well as skills and financial resources having been absorbed into the kinetic war.

4.4 Moving from the temporary enhancement to sustainable capacity

The perception of the assisting entities who were consulted in this research is that the conflict has resulted in enhancements to both their own and Ukrainian capacities and capabilities:

- Key improved capabilities of the organisations who were providing assistance to Ukraine are the development of new defensive tools and techniques; an improved understanding of the threat; and a greater understanding and experience of approaches to providing cyber-defence assistance.
- It is perceived that key improved capacities for Ukraine include upskilling (noting that challenges remain around the number and retention of trained experts); knowledge transfer; and the development of intelligence and public-private partnerships.[9]

Our dialogue found general consensus that, even if the kinetic conflict comes to an end, there is likely to be a protracted cyber conflict. Similar views are expressed in related literature, that cyber operations are likely to continue 'just as offensive cyber operations precede an armed conflict' (Levite 2023). Ukrainian sources suggest that this is also the Ukrainian expectation, with Yurii Shchyhol, head of the Ukrainian State Service of Special Communications, stating 'Even after our victory on the ground, we understand that the cyberwar will not cease, and they will persist in attacking our systems' (Sorokin 2023).

As the conflict continues there is concern about the sustainability of the support and the longevity of the capacities and capabilities developed by Ukraine, particularly if there were to be a transition to reduced external support. Some of the assistance delivered results in a temporary capability enhancement: i.e. provision of capability for a fixed time to fill an immediate gap, which will not necessarily result in a sustained longer-term capacity that Ukraine can deliver itself. The tasks aimed at embedding the capability in such a way that the nation can continue to possess it after the initial provision are not necessarily the same as those undertaken when providing immediate support.

Some support programmes directly aim to create longer-term capacity impacts by supporting the development of CI standards, legislation and strategies, and training programmes. For example, the United States Agency for International Development (USAID) Cybersecurity for Critical Infrastructure in Ukraine Activity has objectives of 'improving the enabling environment for cybersecurity, strengthening Ukraine's cybersecurity workforce, and stimulating market development to promote Ukrainian cybersecurity products and services' (USAID 2023). For internal Ukrainian capacity, how to retain and fund the necessary cyber defence workforce in the long term is a key challenge, in particular given concerns around how attrition (due to skilled people leaving the country or being conscripted to the kinetic fight) will affect the IT and cybersecurity sectors in the country.

While there is more that can be done to enhance Ukraine's own longer-term capacity, ongoing external support is likely to be needed. The approach therefore needs to be two-pronged: building up internal capacity and capability, and sustaining the external support that is likely to be needed in a way that is politically, economically and commercially viable.

There is concern about how to sustain the external support, particularly as the 'outrage factor' fades, and begins to compete with the commercial interests of private-sector organisations. The longer the conflict continues, the more it may be regarded as a cost to private-sector assisting entities, making it harder to justify the benefits and commercial viability to business leaders. Furthermore, there is a risk that resources may be called to other parts of the world to address new situations, to the detriment of Ukraine. There is currently a lack of understanding of the impact and necessary mitigative actions if economic incentives or political factors mean companies withdraw their licences for technologies and cloud services and their remote analytical support.

Therefore, there is a need to develop long-term sustainment strategy that considers: the development of foundational internal capacities and their longevity; the lifecycle of, and incentives for, assistance and how to ensure that this remains viable; and how to transition from reliance on external support to greater reliance on internal capability in the sustainment phase and into the future. This dialogue identified that greater coordination may be a key factor in sustaining external support: more efficient and transparent procurement processes, and identification of roles and of who bears the cost over time. As noted, it is important that any coordination efforts retain the benefits of agility.

Any strategy will also need to take into account the Ukrainian willingness to invest in cybersecurity, which will compete with the urgent need to rebuild national infrastructure or to invest in other elements of its digital economy. Strategy must also take into account the ways in which Ukraine intends, or would like, to evolve its appetite to adopt particular types of cybersecurity technology or processes in the long term. In developing such a strategy, it will be important to understand the extent to which there may be longer-term negative consequences of assistance, which, in bolstering capability in the short term with new technologies and resources, may potentially harm the Ukrainian cybersecurity ecosystem, local supply chains and associated capacities.

Sustainment strategies will need to be able to evolve in line with the balance of capability. The intent and capability of Russia, and how these balance against potential changes to the capability in Ukraine, are currently shrouded in uncertainty. As noted, it is possible that internal capacity and capability in Ukraine may degrade over time as a result of attrition. The capability of Russia and the extent to which it is impacted by factors such as the emigration of technology professionals and international technology sanctions (Hüsch and Jarnecki 2023), is difficult to identify. How to retain parity in a way that is politically, economically and commercially sustainable when Russia may ultimately have more resources to call on is a major challenge.

The community needs to be able to anticipate and be prepared for potential changes in Russian cyber strategy. The offensive cyber strategy so far appears to have focused mainly on damaging the relationship between citizen and state through disruption backed by disinformation and combat support. The extent of successful cyberespionage is difficult to determine.[10] Russian strategy may yet evolve against Ukraine, or to target other actors outside of Ukraine, in particular those supporting assistance or logistically important to the conflict. Our dialogue recognised that future cyberattacks are unlikely to be limited to infrastructures located in Ukraine; wider supply chains and the infrastructures and economies of sympathetic states have already been targeted.[11] It is critical that Ukraine and the international community are able to take account of such evolutions in sustaining cyber-defensive capability.

4.5 Implications for other countries

4.5.1 Context matters

Our expert dialogue has identified contextual factors, specific to this case study of the Ukrainian cyber defence, which may have influenced the balance of Ukrainian and Russian capability, as well as the effectiveness of international assistance. It is important that these factors are recognised, since they may also impact the broader applicability of the lessons learned.

Firstly, multiple sources, including claimed views of Ukrainian experts, suggest that the Ukrainian experience of several major cyberattacks in the months leading up to the invasion, including 'the largest attack in 17 years' against state authorities on 14 January 2022, meant that Ukraine was better prepared for cyber defence in conflict by the time of the invasion.[12]

Secondly, because Ukraine had been a prime target of Russian cyberattacks for years, some companies had already established presence to assist and to gain visibility and knowledge of sophisticated new threats. This meant that a number of pre-existing relationships and networks could be leveraged.

Thirdly, the mutual outrage and interests of private sector organisations and the public sector aligned to create a collective will to act rapidly. This was despite some challenges created by a lack of coordination or preparedness to mobilise public-private partnerships on the part of the assisting community.

Fourthly, while Russia's offensive cyber capability and intent is difficult to identify precisely, the lack of targeted advanced cyberattacks in the early stages of the conflict created a window of opportunity for Ukraine's defensive position to be further strengthened, including with international support.

Reflecting on what lessons can be learnt by other states seeking to prepare for public-private collaborations at pace should incidents occur, the following is observed:

- As noted, in the case of Ukraine, the community may have benefited from the contextual factors (above) that eased the path to assistance in the early months following the invasion, however, these cannot be relied on as the basis for this type of assistance in general.
- Certain of these contextual factors are specific to this conflict: the alignment of the mutual interests of the private and public sectors; the already established presence of assisting private companies in Ukraine; and the window of opportunity for Ukraine to strengthen its defensive position as a result of Russia's initial offensive strategy. This lends criticality to the need to identify approaches that ensure cyber defence and international assistance can be achieved in potentially very different future situations.
- There are concerns about the sustainability of the assistance provisions in a prolonged conflict, particularly if private-sector incentives to support were to alter, or assistance resources were to be required elsewhere in the world. This would in effect add additional context which could reduce capacity support.[13]

4.5.2 Assistance mechanisms are needed to achieve pace and agility

As described, certain conditions specific to this conflict may have eased the path to assistance. The Ukrainian private-public assistance approach in its current form, as well as being potentially fragile in the prolonged Ukrainian conflict, cannot be relied on to stand up in other situations where aggressors' tactics may differ, and private and public incentives may not align in the same way (in particular, where the outrage factor is not as

intense, or companies' commercial or political interests inhibit involvement).[14] This drives a critical need to identify the extent to which the effort would be replicable in potential future cases of cyber aggression in other parts of the world. This includes the potential immediate spread of the current cyber conflict, e.g. within NATO; and other potential theatres of war, particularly in countries where there is a commitment to support allies. Participants in our research agreed that the community should develop and test a range of scenarios to explore this issue.

To ensure the ability of public-private assistance partnerships to mobilise as necessary in potential future situations, there is a need to develop coherent international cyber defence assistance mechanisms. Critical requirements (which are detailed in the 'Recommendations' section) are: the development of necessary relationships amongst assisting entities and in the potential recipient countries; the definition of roles and responsibilities for assistance, including who bears the cost over time; and the definition of rules of private-public engagement, including any necessary legal top cover. In practical terms, informal, threat-led coordination networks, the development of a crisis playbook for requesting and delivering cyber defence assistance, and scenario exercising may be valuable approaches to meeting these needs.

The effective absorption of crisis assistance requires a level of internal cybersecurity capacity to be in place in the recipient country. There is a need to identify the minimum baseline of national cybersecurity capacities that is necessary. This baseline should inform capacity and capability-building efforts globally, while understanding where any potential future recipient country stands in relation to this baseline should contribute to shaping the assistance offer. There is also a need to understand how specific contextual factors in other potential scenarios must impact on shaping the assistance offer and on the ability to absorb assistance.

A key example is whether the recipient of assistance is legally or technically able to operate in a global cloud environment, as the cloud is becoming a *de facto* standard for remotely handling cyber threat intelligence and delivering threat monitoring analytics. In the case of Ukraine, data sovereignty legislation that prohibited hosting national data in third-party cloud environments had to be suspended before cloud migration could be enacted. The view expressed by cloud-based assistance providers during our dialogue was that this cloud migration was essential to limiting harm: greater harm could have resulted had Ukraine not accepted this particular assistance, as critical data and back-ups kept on premises could have been lost or corrupted through cyber or kinetic attack. The nature of the assistance, in many cases, will dictate if it is possible to deploy capabilities locally or necessarily remotely (e.g. if human analysts are needed but unable to travel to a conflict zone, then cloud approaches enable assistance otherwise unachievable with the supplier). For potential future recipient countries with strong data sovereignty policies, there may be a need to consider now how assistance would need to be provisioned, so it can quickly be delivered.

4.6 Summary of key observations

- **Key to success is the strength of existing networks and relationships.** There is a general consensus that experiences so far have underlined the importance of

trusted personal and institutional relationships. In Ukraine, the relationships of external private-sector organisations, with entities in the country as a result of pre-existing collaboration and presence, facilitated immediate and effective assistance, where there may otherwise have been challenges exacerbated by language and cultural differences and a lack of familiarity with key personnel. The strength of the relationships and trust between public and private assisting entities, as well as between private-sector companies, was also important in facilitating agile action. Ensuring that the necessary relationships are developed and sustained in preparation for future situations is critical.

- **Coordination is needed, but agility must be retained.** There is a need to coordinate the roles and responsibilities of the various entities involved in providing immediate cyber defence assistance. There is a clear lack of understanding and inventory of what assistance is being provided to Ukraine, and the time horizon of that assistance. It is important for Ukraine, however, that advantageous elements of the approach thus far are retained: the somewhat diffuse actions of the private sector, with a limited level of coordination by governments and also through volunteer efforts[15] have been sufficiently agile to move at the speed of the cyber aggression. Recent initiatives have sought to put in place coordination approaches, in particular through the formalisation of the Tallinn Mechanism to coordinate civilian cyber assistance to Ukraine (US Department of State 2023).

  Coordination models will need to account for the material ways in which the incentives of the private sector differ from the drivers of government; for example, the ECCRI expert workshop of 2023 noted that 'Industry is ultimately beholden to shareholders and driven by market forces; these incentive structures are distinct from the drivers of government and need to be acknowledged when assessing private sector roles and responsibilities' (Grossman et al. 2023). The potential implications of reliance on the private sector in these roles also need to be taken into account; the same ECCRI report describes the concern of expert participants that 'blurring the lines of responsibility between government and industry can be advantageous in the short-term but can have profoundly destabilising effects in the long run. For example, the US reliance on private military and security companies in Iraq in the 2000s raised significant questions about the duties and legal responsibilities of the host state'.

  Furthermore, government stakeholders in our dialogue described the challenges they face in private sector-led initiatives, including the need to still be able to monitor success and demonstrate deliverables. Coordination models will also need to account for differences in government and private resources and capability to take on roles in providing assistance and measuring success. Processes will need to be matured that can help support speed of deployment. Such processes will need to enable decisions to be made around what cybersecurity capacities to prioritise for enhancement, and these will necessarily involve both assisting countries and the recipient country. These decisions are likely to necessitate technical understanding as well as strategic expertise, identifying both and ensuring lines of responsibility that are operationally effective will be imperative to the processes if speed is to be achieved.
- **Recipient country cybersecurity skills and processes are critical**. The importance of people and process to cyber resilience has been underlined, highlighting the

criticality of education and training as a key component of building sustainable cybersecurity capacity. In order to absorb immediate technical assistance, and also to sustain the benefits of capability enhancements into longer-term internal capacities, there is a need for a cybersecurity workforce in the country that has the necessary skills and experience and is large enough to be resilient to wartime attrition factors.

5. Recommendations

The following recommendations may be important for the sustainment of cyber-defensive capability in the context of the ongoing Ukraine conflict, and for preparing for potential future situations elsewhere in the world:

- **Identification of a cybersecurity-capacity minimum baseline for effective capability absorption.** There is a need to identify the minimum baseline of national cybersecurity capacities that is necessary for a recipient country to effectively absorb assistance. Clearly the application of this baseline would be context-specific. It would be beneficial for the baseline to be correlated with existing cybersecurity capacity assessment models, such that national cybersecurity capacity assessments can be used to identify potential shortfalls in a nation's crisis assistance-absorption ability. Similarly, the baseline should inform capacity-building efforts globally. This baseline could also be used to shape assistance offers in the future, since it can indicate the likelihood of successful impact of relative packages.

  Research is needed to support the development of this minimum baseline. Through the preliminary findings of this case study we have begun to identify potential elements: key capacities important for the effective absorption of assistance. In particular, the availability of sufficient numbers of skilled personnel, with established roles and responsibilities for cybersecurity is critical, while an awareness of the nation's current security posture, digital-infrastructure security and security tools, is needed to support effective assistance requests in the case of a crisis. The importance of developing strong networks and relationships between a range of different types of party has also been highlighted, and consideration must be given to how a minimum baseline of capacity would account for this need.
- **Development of a crisis playbook for requesting and delivering external assistance.** There may be value in a maintained and continuously evolving crisis playbook that covers both requesting external assistance and delivering it, noting that this will need to be able to cater for different countries with very different assistance needs. This should cover rapid needs assessment (understanding of what capability is already in place and what is needed as a priority) and how this shapes the offer of assistance. It would also be valuable to cover how to respond as the threat increases in pace, scale or sophistication, prior to large-scale assistance requirements. It is the authors' opinion that the development of this playbook will require a multi-stakeholder approach including all sectors that are likely to be involved in assistance (as otherwise it may not take account of the operational needs of all involved). Further, certain conflicts may involve humanitarian aid organisations, and therefore they should be included.

- **Development of crisis scenarios.** Consideration should be given to identifying a set of potential crisis scenarios affecting different countries and to using these to help develop and test the cybersecurity-capacity minimum baselines, and to inform the crisis playbook.

  The conflict in Ukraine has highlighted key crisis capabilities that need to be reflected in these scenarios. This includes the ability to operate in a hybrid conflict: participants reported that kinetic attacks have been used to disrupt internet infrastructure, such as through the cutting of internet cables, and there are also concerns about the potential impacts of physical attacks on data centres. Additionally, electronic warfare (to disrupt the stability of communications) and disinformation campaigns have been used to shape the kinetic battle (Sorokin 2023).

  It is also critical that crisis scenarios account for the interconnectivity of communications and information infrastructure and the interdependence of digital services and providers (for example, the reliance of CI on private internet infrastructure). These factors can cause risk to aggregate and, as such, need to inform the prioritisation of assistance. Although they can also create resilience, as has reportedly been the case for Ukraine's internet infrastructure and routing due to widespread connectivity to networks outside the country (Tomé, Belson, and Berdan 2023).
- **Development of strategies (and supporting research) for sustained capacity and capacity-building.** There is a need to develop strategy for sustaining long-term capability following immediate assistance. Strategy will need to consider: the development of foundational internal capacities and their longevity; the lifecycle of, and incentives for, assistance and how to ensure that this remains viable; the recipient country's plans for investment and evolution in cybersecurity; and how to transition from reliance on external support to greater reliance on internal capability in the sustainment phase.

  Sustainment strategies will need to be able to evolve in line with changes to threat actor strategy and the balance between evolving threat actor and defender capabilities. This should inform ongoing sustainment of internal capability and assistance for Ukraine, as well as informing both long-term capacity-building and immediate assistance approaches for other situations.

  Critical to sustaining funding by governments and private-sector companies will be the ability to measure the success of initiatives. Presenting the 'business case' for assistance, and quantifying the impact of assistance interventions, will help justify sustainment of assistance; such analysis will become increasingly valuable if motivations to assist change or competing assistance needs arise in other situations. There is a need to identify the relevant metrics and necessary data for evaluating success.
- **Formation of an assistance-coordination network.** To support agile and informal immediate-assistance cooperation and implement the crisis playbook, it may be valuable to form a coordination network that gathers to consider emerging threat scenarios. This could help to build the relationships and understanding of roles necessary to support immediate assistance, regardless of the aggressor and assisted country in future situations.[16]

  Coordination models will need to be based on an understanding of the comparative advantages to the recipient, and the motivations of various private-sector entities, including their technical capabilities, existing relationships, footprints in different regions of the world, and competition with each other in the commercial market.

They will also need to be shaped by geopolitical position and the capabilities of different governments (and particular ministries within governments) and multinational organisations: their relationships with, and ability to contract, private-sector technology companies, and the resources available to them. In developing coordination models, there may be lessons to draw from models for the provision of other types of coordinated assistance, such as kinetic defence, humanitarian aid, and disaster response.

- **Definition of (international) ground rules for private-public engagement.** For sustained assistance in the current protracted conflict, as well as to ensure that private-sector support is viable in potential future situations, the ground rules for engagement need to be defined and mechanisms put in place to enact them. This will need to include: an understanding of who bears the cost of assistance over time; identification and management of potential liability risks to responders from being involved (including legal protections to ensure that assistance is viable); and, potentially, development of Public-Private-Partnership (PPP) models for contracting the private sector.

  However, it is noted that a strength observed in the Ukrainian support activities was the agility with which elements of the private sector were able to respond. Consideration should be given to protecting and retaining the necessary agility when designing procurement frameworks; a pivot towards an administrative-heavy framework which precludes agile response outside the framework would be detrimental to the overall resilience effort.

The current situation in Ukraine will continue to evolve, and any future situations will undoubtedly have their own unique characteristics to address. It is therefore critical that, in implementing these recommendations, the community is able to benefit from continuous and collective refinement of approaches in line with lessons learned, and to take account of evolutions in the threat landscape and the impact of varying contextual factors in different conflict situations.

6. Conclusion

There is a sentiment that this is the first real test[17] of the ability of a single state, supported by assistance from the international community security and digital sector, to rapidly put up a cyber defence at national scale against a sophisticated cyber aggressor in the context of a war. Further, that the experience has shown that with the right capacities, will and contextual conditions, it is achievable.

It is important to temper statements on the effectiveness of the Ukrainian cyber defence and lessons learned for other situations against a number of contextual factors specific to this conflict that must be taken into account; these factors are discussed earlier in the paper. There have already been many challenges in mounting the defence, from which lessons must be learned both for sustainment of the Ukrainian defence in the ongoing conflict, and for potential future conflicts elsewhere in the world. It is also important to recognise that the conflict is ongoing, and potential changes in respective capabilities, as well as Russian strategy and cyber operations of both sides, could yet alter the balance. The European Cyber Conflict Research Initiative (ECCRI) similarly reported expert discussion on potential evolutions in capability and strategy, including the possibility that 'more disruptive or destructive cyber attacks' might 'occur in future, as Russian cyber actors continue

to develop their access to Ukrainian information infrastructure', and the possibility of Russian employee burnout as a result of the high operational tempo (Kaminska, Shires, and Smeets 2022). That said, we can already begin to learn lessons on how to enable future private-public initiative in support of protecting national public infrastructures.

Notes

1. Mandiant reported observing 'more destructive cyberattacks in Ukraine during the first four months of 2022 than in the previous eight years with a notable spike in activity at the start of the invasion' (Google 2023). Threat reporting by Microsoft, Cisco and other companies have also shown the significant cyber dimension to the conflict (Willett 2022).
2. For assumptions about Russia's cyber capabilities, see Voo et al. (2020).
3. English translation by Keir Giles, see reference.
4. Scholars including Thomas Rid (2022) and Lucas Kello (2017) have also explored the possibility of cyberwar, although this is beyond the scope of this article.
5. A similar discussion can be found in Haklai (2023, 662). See also Steele (2023).
6. This coheres with Dunn Cavelty's discussion about cybersecurity and PPPs (2015), which notes that a key function is information sharing.
7. Consistent with the challenges of PPP reported in research such as (Haklai 2023), in this case the challenge of misaligned incentives appears to have been minimal.
8. This paper's findings on the challenges of defining roles and responsibilities, liability, and alignment of incentives, cohere with Haklai's theories (2023) on the challenges of cybersecurity PPPs.
9. These beliefs have not been verified by representatives from Ukraine.
10. It has been argued however, that, based on a limited number of known cases, cyber-derived intelligence seems to have 'yielded little military benefit' for targeting decisions (Bateman 2022). Still, there is not sufficient data to yield a conclusion to the debate, and there must be some perceived benefit as the campaigns continue to be deployed.
11. See for example (Microsoft 2022).
12. See for example Sorokin (2023).
13. However, in the case of Ukraine, our dialogue suggested that during the early stages of urgency, many critical assistance capabilities and relationships were built, which, it is anticipated, will support the continued provision of assistance.
14. For a discussion of potential challenges, see Christensen and Lund (2017) and Dunn Cavelty and Mauer (2007).
15. E.g. through the Cyber Defence Assistance Collaborative (Aspen Institute 2023).
16. The ECCRI 2023 workshop report concurs that coordination models may prove more useful than 'top-down collaboration vehicles' and cites 'the UK Industry 100 programme operated by the NCSC and the CyberPeace Builders programme' as potentially relevant examples (Grossman et al. 2023).
17. It is well known that there have been cyber aspects of conflict and terrorism for over 20 years, but not involving international cooperation of the scale being witnessed in the current Ukraine-Russia conflict.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Dr Louise Axon is a Research Fellow in the Global Cybersecurity Capacity Centre and the Cybersecurity Analytics Group at the University of Oxford. She has a DPhil in Cybersecurity from Oxford. Her research interests include cybersecurity capacity building, systemic cyber-risk, and developing

operational cybersecurity approaches for emerging threats. She supervises cybersecurity student projects and teaches courses at the University, and is a member of the World Economic Forum Expert Network.

Dr Jamie Saunders is a strategic security consultant. He is a Fellow of the James Martin School at the University of Oxford and a Fellow of the European School of Management and Technology's Digital Society Institute. He is a member of the UK Government's Expert Advisory Group on Cyber Resilience, a member of the Advisory Group of the UK's Association of Insurance and Risk Managers in Industry and Commerce, and works with a number of digital security start-ups in the UK, US and Japan. Jamie retired from the Board of the National Crime Agency in 2017 after 29 years of government service in the UK.

Dr Patricia Esteve-González is a Senior Research Associate at the Global Cyber Security Capacity Centre, University of Oxford. She has a PhD in Economics and her research interests focus on the role of institutions and the mechanism design of their policies. Her published and ongoing research uses theoretical and empirical methodologies in a variety of contexts, including cybersecurity capacity.

Julia Carver is a DPhil candidate in International Relations at the University of Oxford, and a Research Associate at the Global Cybersecurity Capacity Centre. Her work engages across disciplines (strategic studies, IR, development studies, and political geography) and seeks to understand to understand the evolution of 'cyber-IR' and strategic thinking in the contemporary 'information age'. Julia is a Special (Stipendiary) Lecturer in Politics for Magdalen College, teaching International Relations and the Practice of Politics, and a European Cyber Security Fellow at the European Cyber Conflict Research Initiative.

Professor William H. Dutton is Director of the Portulans Institute, and a Fellow at the Oxford Internet Institute (OII) and the Oxford Martin School at the University of Oxford, where he supports Oxford's Global Centre for Cyber Security Capacity (GCSCC). He was the founding director of the OII, the first Professor of Internet Studies at Oxford University, and an Emeritus Professor at the University of Southern California. His most recent book is *The Fifth Estate: The Power Shift of the Digital Age* (OUP 2023).

Professor Michael Goldsmith is a Senior Research Fellow at the Department of Computer Science and at Worcester College, Oxford. He studied Classical Languages and Literature and Mathematics and Philosophy at St John's College, Oxford, where he completed his DPhil in Computation. After some postdoctoral posts he became the founding employee of Formal Systems (Europe) Ltd, a small business in Oxford, where he rose to become Managing Director before returning to academia at the University of Warwick Digital Laboratory in 2007, and to the University of Oxford in 2011. His recent research has encompassed a range of projects ranging from highly mathematical semantic models to multidisciplinary research at the socio-technical interface. He is a Co-Director of the Cyber Security Oxford network and of the Global Cyber Security Capacity Centre.

Professor Sadie Creese is Professor of Cybersecurity in the Department of Computer Science at the University of Oxford. Sadie is the founding Director of the Global Cyber Security Capacity Centre (GCSCC) at the Oxford Martin School, where she continues to serve as a Director conducting research into what constitutes national cybersecurity capacity, working with countries and international organisations around the world. She was the founding Director of Oxford's Cybersecurity network, and is a member of the World Economic Forum's Cyber Security Centre's Strategic Advisory Board. Sadie teaches operational aspects of cybersecurity including threat detection and security architectures, and is Course Director for the Saïd Business School's online programme Cybersecurity for Business Leaders.

ORCID

Louise Axon http://orcid.org/0000-0001-5979-7630

References

Aspen Institute. 2023. *The Cyber Defense Assistance Imperative: Lessons From Ukraine*. s.l.: s.n.

Bateman, J. 2022. *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*. s.l.: Carnegie Endowment for International Peace.

Beecroft, N. 2022. *Evaluating the International Support to Ukrainian Cyber Defense*. s.l.: Carnegia Endowment for International Peace.

Bevir, M., and R. Rhodes. 2016. *Routledge Handbook of Interpretive Political Science*. 1st ed. s.l.: Routledge.

Carrapico, H., and B. Ferrand. 2020. "Discursive Continuity and Change in The Time of Covid-19: The Case of EU Cybersecurity Policy." *Journal of European Integration* 42 (8): 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Cattler, D., and D. Black. 2022. "The Myth of the Missing Cyberwar." *Foreign Affairs*, April 6. Accessed December 18, 2024. https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.

Christensen, K. K., and P. Karen Lund. 2017. "Public–private Partnerships on Cyber Security: a Practice of Loyalty." *International Affairs* 93 (6): 1435–1452. https://doi.org/10.1093/ia/iix189

Collier, J. 2018. "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision." *Politics and Governance* 6 (2): 13–21. https://doi.org/10.17645/pag.v6i2.1324

Diesing, P. 2008. *Patterns of Discovery in the Social Sciences*. London: Routledge.

Dunn Cavelty, M. 2015. "Cyber-Security and Private Actors." In *Routledge Handbook of Private Security Studies*, edited by Rita Abrahamsen and Anna Leander, 11. s.l.: Routledge.

Dunn Cavelty, M. 2022. "Cyber-security." In *Contemporary Security Studies*, edited by A. Collins, 422–436. 6th ed. Oxford: Oxford University Press.

Dunn Cavelty, M., and V. Mauer. 2007. "The Role of the State in Securing the Information Age: Challenges and Prospects." In *Power and Security In The Information Age: Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel, 181–182. s.l.:s.n.

The Economist. 2024. "The Cyberwar in Ukraine is as Crucial as the Battle in the Trenches." *The Economist*, March 20. Accessed December 18, 2024. https://www.economist.com/europe/2024/03/20/the-cyberwar-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches.

European Union Agency for Cybersecurity (ENISA). 2024. "Public Private Partnerships (PPPs)." *European Union Agency for Cybersecurity*. Accessed September 20, 2024. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps.

Giles, K. 2022. "Putin Does Not Need to Invade Ukraine to Get his Way." *Chatham House*, January 10. Accessed December 18, 2024. https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

Giles, K. 2023. "Russian Cyber and Information Warfare in Practice: Lessons Observed From the War on Ukraine." *Chatham House*, December 14. Accessed December 18, 2024. https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf.

Global Cyber Security Capacity Centre (GCSCC). 2021. "Cybersecurity Capacity Maturity Model for Nations (CMM)." *Oxford University*. Accessed December 18, 2024. https://gcscc.ox.ac.uk/the-cmm.

Google. 2023. "Fog of War: How The Ukraine Conflict Transformed the Cyber Threat Landscape." *Google Blog*, February 16. Accessed December 18, 2024. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

Grossman, T., M. Kaminska, J. Shires, and M. Smeets. 2023. *The Cyber Dimensions of the Russia-Ukraine War* (Workshop Report). European Cyber Conflict Research Initiative. s.l.: s.n.

Haklai, B. 2023. "Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity." *Texas Tech Law Review* 56:627.

Hathaway, M., C. Demchak, J. Kerben, J. McArdle, and F. Spidalieri. 2015. *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies. Accessed January 3, 2025. https://www.potomacinstitute.

org/steps/index.php/component/content/article/cyber-readiness-index-cri-2-0?catid = 31&Itemid = 101.
Healey, J. 2022. "Preparing for Inevitable Cyber Surprise." *War on the Rocks*, January 12. Accessed December 18, 2024. https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.
Hüsch, P., and J. Jarnecki. 2023. "All Quiet on the Cyber Front? Explaining Russia's Limited Cyber Effects." *Royal United Services Institute (RUSI)*, June 1. Accessed December 18, 2024. https://www.rusi.org/explore-our-research/publications/commentary/all-quiet-cyber-front-explaining-russias-limited-cyber-effects.
International Institute for Strategic Studies (IISS). 2021. *Cyber Capabilities and National Power: A Net Assessment*. s.l.:s.n.
International Telecommunication Union (ITU). 2024. *Global Cybersecurity Index (GCI)*. Accessed January 3, 2025. https://www.itu.int/hub/publication/d-hdb-gci-01-2024/.
Kallas, K. 2023. "Kaja Kallas Says Ukraine is Giving the Free World a Masterclass on Cyber-Defence." *The Economist*, April 17. Accessed December 18, 2024. https://www.economist.com/by-invitation/2023/04/17/kaja-kallas-says-ukraine-is-giving-the-free-world-a-masterclass-on-cyber-defence.
Kaminska, M., J. Shires, and M. Smeets. 2022. *Cyber Operations During the 2022 Russian Invasion of Ukraine: Lessons Learned (So Far).* European Cyber Conflict Research Initiative. s.l.: s.n.
Kello, L. 2017. "Russia and Cyberspace: Manifestations of the Revolution." In *The Virtual Weapon and International Order*, edited by Lucas Kello, 320. s.l.: Yale University Press.
Kostyuk, N., and E. Gartzke. 2022. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine." *Texas National Security Review* 5 (3): 113–126.
Lehdonvirta, V. 2022. *Cloud Empires: How Digital Platforms Are Overtaking The State and How We Can Regain Control*. Cambridge, MA: The MIT Press.
Levite, A. 2023. "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict." *Carnegie Endowment for International Peace*, April 18. Accessed December 18, 2024. https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict?lang = en.
Libiseller, C. 2023. "'Hybrid Warfare' as an Academic Fashion." *Journal of Strategic Studies* 46 (4): 858–880. https://doi.org/10.1080/01402390.2023.2177987
Liebetrau, T., and K. K. Christensen. 2021. "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites, and Spaces." *European Journal of International Security* 6 (1): 25–43. https://doi.org/10.1017/eis.2020.10
Liebetrau, T., and L. Monsees. 2023. "Assembling Publics: Microsoft, Cybersecurity, and Public-Private Relations." *Politics and Governance* 11 (3): 157–167. https://doi.org/10.17645/pag.v11i3.6771
Mandiant. 2023. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology." *Google Blog*, November 9. Accessed December 18, 2024. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.
Matishak, M. 2021. "Russia Could Launch Digital Offensive Against Ukraine, Administration Official Warns." *The Record*, December 6. Accessed December 18, 2024. https://therecord.media/russia-could-launch-digital-offensive-against-ukraine-administration-official-warns.
McCarthy, D. 2018. "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order." *Politics and Governance* 6 (2): 5–12. https://doi.org/10.17645/pag.v6i2.1335
Pestarino, C. 2023. "57% Surge of Cyberattacks in Europe Flagged by DIGITAL SME Report." *European Digital SME Alliance*, October 17. Accessed December 18, 2024. https://www.digitalsme.eu/57-surge-of-cyberattacks-in-europe-flagged-by-digital-sme-report/.
Przetacznik, J., and S. Tarpova. 2022. *Russia's War on Ukraine: Timeline of Cyber-Attacks*. s.l.: European Parliamentary Research Service. Accessed December 18, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.
Reuters. 2020. "Ukraine Says Faces Almost Daily Hacker Attacks." *Reuters*, December 18. Accessed December 18, 2024. https://www.reuters.com/business/media-telecom/ukraine-says-faces-almost-daily-hacker-attacks-2020-12-18/.

Rid, T. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. 2022. "Why You Haven't Heard About the Secret Cyber War in Ukraine." *The New York Times*, March 18. Accessed December 18, 2024. https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html.

Sanger, D. E. 2022. "Arming Ukraine: 17,000 Anti-Tank Weapons in 6 Days and a Clandestine Cybercorps." *The New York Times*, March 6. Accessed December 18, 2024. https://www.nytimes.com/2022/03/06/us/politics/us-ukraine-weapons.html.

Sorokin, O. 2023. "Ukraine May be Winning "World's First Cyberwar"". *The Kyiv Independent*, August 4. Accessed December 18, 2024. https://kyivindependent.com/ukraines-cyber-chief-says-kyiv-is-winning-worlds-first-cyberwar/.

Steele, G. 2023. "Data and Public-Private Partnerships are the Future of Cybersecurity." *World Economic Forum*, January 16. Accessed December 18, 2024. https://www.weforum.org/stories/2023/01/data-and-public-private-partnerships-cybersecurity/.

Thorne, S. E. 2020. "Applied Interpretive Approaches." In *The Oxford Handbook of Qualitative Research*, edited by P. Leavy, 143–166. s.l.: Oxford University Press.

Tomé, J., D. Belson, and K. Berdan. 2023. "One Year of War in Ukraine: Internet Trends, Attacks, and Resilience." Cloudfare, *The Cloudflare Blog*, February 23. Accessed December 18, 2024. https://blog.cloudflare.com/one-year-of-war-in-ukraine/.

United States Agency for International Development (USAID). 2023. USAID *Cybersecurity for Critical Infrastructure in Ukraine: Cyber Sector Update*. s.l.: USAID. Accessed December 18, 2024. https://cybersecurity.sumdu.edu.ua/wp-content/uploads/2023/10/usaid-ukraine-cci-cyber-sector-update-2023-q3.pdf.

US Department of State. 2023. "Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine." *US Department of State*, December 20. Accessed December 18, 2024. https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/.

USAID. 2022. *Press Release: USAID Safeguards Internet Access in Ukraine through Public-Private-Partnership with SpaceX*. s.l.: USAID. Accessed December 18, 2024. https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex.

Voo, J., I. Hemani, S. Jones, W. DeSombre, D. Cassidy, and A. Schwarzenbach. 2020. *National Cyber Power Index* 2020. s.l.: Harvard Kennedy School Belfer Center for Science and International Affairs. Accessed December 18, 2024. https://www.belfercenter.org/publication/national-cyber-power-index-2020.

Walker, K. 2022. "Helping Ukraine." *Google Blog*, March 4. Accessed September 20, 2024. https://blog.google/inside-google/company-announcements/helping-ukraine/.

Willett, M. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival* 64 (5): 7–26. https://doi.org/10.1080/00396338.2022.2126193

Yin, R. 2017. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: Sage.