Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences

Dan Black

March 2023

IISS
The International Institute
for Strategic Studies

Contents

Executive Summary

Despite expectations to the contrary, cyber defence, not offence, has been the story of Russia's war against Ukraine as it enters its second year. Shattering concepts of offence dominance, Kyiv's cyber-defensive effort has shown that a strong and layered cyber defence can be mounted against a well-resourced and highly capable adversary. The preeminent question in policy debates has been: 'How can other states replicate Ukraine's success?'

This is a complex issue. The fog of war has been even thicker on the defensive side of the war, with many Ukrainian activities necessarily shielded from public view for operational security. Yet careful examination of the available evidence would suggest that the primary lessons lie less in what Ukraine has done and more generally in its superior capacity to adjust to various aspects of Russia's cyber offensive. Institutional adaptations such as legislative change in Ukraine and measures taken to garner public- and private-sector support have driven much of Kyiv's defensive success. At this stage of the war, it is uncontroversial to argue that Ukraine has decisively won the adaptation battle in cyberspace.

This adaptive capacity was engineered well in advance of the February 2022 invasion. As this paper details, underlying Ukraine's ability to make agile decisions and outmanoeuvre Russia's cyber forces is the culmination of years of experience, investment and high-level policymaker attention dedicated to improving the country's cyber defences. Kyiv's familiarity with Moscow's approach to information confrontation and the former's years of defending against network attacks are equally crucial. The Ukrainian experience hence teaches a twofold lesson that while early contestation and defensive reinforcement can undermine the adversary's plans and intentions, sound defensive fundamentals are required to sustain those advantages.

There are also other pressing policy questions. The first is: how durable is the 'Ukrainian model' as the war enters another year with seemingly no end in sight? To date, Kyiv has deftly marshalled its defensive resources and orchestrated diverse forms of external support to stem the Russian cyber offensive. However, concerns of 'fatigue' setting in are just as consequential to Ukraine's cyber defence as they are in other domains of war. After all, defensive reinforcements are not limitless, and competing priorities or emerging crises elsewhere in the world could divert attention and resources away from the Ukraine front. Changing economic conditions could also stem crucial private-sector support for Ukraine's cyber defence. Moreover, notwithstanding popular narratives about the ineptitude Russia's cyber forces have displayed so far, they remain highly skilled and have shown that they are tactically adaptable. We should therefore not underestimate Russia's cyber programme nor think that its hitherto shortcomings will persist. Governments should therefore undertake proactive efforts to prioritise critical collective-defence measures to ensure their long-term sustainability. Notably, there are significant opportunities to be realised here to bolster existing multilateral mechanisms and better coordinate public- and private-sector commitments.

A second question is: what more can be done to bolster Ukraine's cyber defences? It is easy to get carried away by triumphalism about Kyiv's cyber successes and the vital role that Western support has played in this regard. But many aspects of this effort have been improvised. Governments and private firms assisting Ukraine have been thrust into the war with limited planning and forethought about Ukraine's specific needs or how to respond as part of a collective-defence architecture. This means that to truly learn the appropriate cyber-defence lessons from the war, we must approach Ukraine's defensive success with a critical eye. There remain critical gaps, unmet needs and significant opportunities for improvement.

The third question is: how relevant would the Ukraine model be for future conflict scenarios, such as a potential Chinese invasion of Taiwan? Here, the takeaways are murkier. Broad-based and sustained investments to boost visibility, detection and resilience will surely help position Taipei to win its own adaptation battles. But we also must recognise that China is likely to exercise cyber power in fundamentally different ways than Russia. Unique challenges such as Taiwan's geographic position and Chinese cyber and economic power suggest different approaches and partners may be required to bolster Taipei's cyber-defence posture.

Background

For a war characterised by the unprecedented public availability of intelligence, remarkably little remains understood about what has happened in the cyber domain of the Ukraine war. Over a year has passed since Russia's brutal and unjustified invasion of Ukraine. Yet details of the specific targets, impacts and desired outcomes of the Kremlin's cyber operations remain largely inscrutable even to the closest of outside observers. While Ukraine's national cyber authorities and Western cyber-security companies have made concerted efforts to detail Russian network attacks to inform the public, policymakers and the cyber-security community, publicly reported incidents are only the tip of the iceberg of a multi-pronged cyber campaign unprecedented in scale and intensity.

However, even with limited insights into the cyber dimensions of the war, it is clear that Kyiv has had great success fending off Moscow's cyber offence. Despite Russia possessing one of the world's most technically proficient and experienced cyber forces, coupled with a deep familiarity with Ukrainian networks from years of priority targeting of the country's critical information infrastructure (CII), Ukraine has orchestrated a strong, layered and resilient cyber defence.

Top Western officials have drawn special attention to Ukraine's ability to withstand Russia's sustained cyber pressure. Jeremy Fleming, director of the United Kingdom's Government Communication Headquarters, remarked in August 2022 that Ukraine had carried out what was arguably 'the most effective defensive cyber activity in history'.[1] Similarly, the head of the UK's National Cyber Security Centre argued that Ukraine 'has provided us with the clearest demonstration that a strong and effective cyber defence can be mounted, even against an adversary as well prepared and resourced as the Russian Federation'.[2] Various other Western voices, including those from the United States, European Union and NATO, have echoed variants of this sentiment.[3]

These accolades are not merely policy rhetoric. The months past saw the Ukrainian model being factored into Euro-Atlantic states' security and defence policies. At the June 2022 NATO Summit in Madrid, the Alliance announced that it would begin to build a virtual rapid-response capability with an eye towards using NATO to coordinate national assets and respond to significant campaigns of malicious cyber activity like the one seen in Ukraine. There were similar efforts within EU states to adapt their existing cyber rapid-response teams to remotely support Ukraine.[4] Kyiv's defensive efforts are highly likely to inspire reforms of other national and multinational cyber-defence programmes given the benefits provided for threat analysis, resilience of CII and flexible response capacity.

Enabling these structural adaptations to succeed will require substantive details. What factors account for Ukraine's heretofore effective cyber defence? How best can others adapt existing strategies and policies to build necessary resilience and seize the initiative away from a well-prepared and resourced adversary? We do not have precedents or analogues beyond Ukraine to help us think through what a sustained and intensive cyber defence effort looks like in practice. How we understand the finer details will have outsized implications for how governments and private industry prepare for the next crisis.

Scope of Paper

While various actors have exploited cyberspace during Russia's war in Ukraine, this analysis specifically looks at Russia's offensive cyber operations (OCOs) and their supporting elements against Ukraine's critical information infrastructure. To this end, the report considers events between March 2021, when Russia's war preparations began, and November 2022, where the war slowed for winter.

By focusing on OCOs, this paper includes publicly reported instances of cyber operations attempting to manipulate, disrupt, deny, degrade or destroy computers or networks or the information resident on them. This is because courses of action leveraging offensive cyber capabilities have been the most visible and reported aspect of Russia's cyber campaign. The paper provides a thorough look at how Moscow has sought to use cyber as a force multiplier for its war-fighting effort. The analysis also considers the nature of Russia's access operations, which have provided the basis for sabotage teams to effectively conduct OCOs. Correspondingly, this paper excludes the analysis of entire categories of Russian cyber operations such as the acquisition of covert infrastructure, intelligence collection and cyber-enabled influence operations, even though they too have been central to Russia's wartime efforts.

This report also delves into specific aspects of CII – the databases, systems, services, networks and infrastructure that underpin physical critical infrastructure.[5] There is a wide variance in what nations define as critical infrastructure, leading to ambiguity in how different countries perceive CII.[6] To compound matters, there are only a few national concepts inclusive enough to fully consider the range of CII elements whose loss or compromise could be detrimental to national security, economic or social structures, or the functioning of the state. For example, it has become common practice to distinguish between government and critical infrastructure networks. But some government networks have been vital to maintaining communications between Ukrainian officials and ensuring continued protection of Ukrainian citizens from Russian attack. The Kremlin itself has recognised this importance, with about a quarter of its OCOs targeting Ukraine's government organisations in the first nine months of the war.

There is also a tendency to conflate CII with operational technology (OT) as well as industrial-control systems that operate, control and monitor industrial processes in critical infrastructure. But this precludes a significant part of the attack surface that requires attention. Incidents such as the Colonial Pipeline ransomware attack underscore that information technology (IT) network attacks can result in significant disruption without the perpetrator gaining access to the target's OT networks. And the rise in supply-chain compromises of technology-service providers in recent years has further emphasised the complex web of dependencies and global suppliers underpinning national CII assets. The point is that CII is defined by a considerably different set of assets and considerations than those typically conceived under the physically rooted concept of critical infrastructure protection. This analysis therefore adopts a more cyber-specific definition of what is 'critical', accounting for the fundamental dependencies and tight coupling between common forms of information infrastructure and indispensable state functions.

Chapter One: Russia's Cyber Offensive

The failure or success of cyber defences, however well planned, is relative to the offensive performance of the opponent. Consequently, in order to analyse what has contributed to the success of Ukraine's cyber defence, it is first necessary to examine Russia's approach to offensive operations and the tactical adaptations its cyber forces have made to operate under conditions of war.

This section explores Russia's cyber offensive through various phases that mirror its conventional military campaign. In each phase, it can be seen that the pattern of cyber operations and the related exploitation of Ukraine's CII assets shifted in line with Russia's evolving war aims. There was an identifiable evolution in the operational priorities, target selection and tactics of Russian cyber actors that corresponded with broader changes in the correlation of forces and the difficulties Russia faced in a fast-paced and highly contested operating environment. Assessing Russia's cyber offensive through the lenses of the different phases also allows for a study of Moscow's cyber activities under different wartime contexts. The opening phase of the war illuminates Russia's envisioned use of cyber operations to shock and surprise in support of its invasion force, whereas the subsequent phases hold insights into Russia's employment of cyber units in a protracted war of attrition. Tracking these changes over time provides a unique lens into the flexible role cyber operations may play in future conflicts and the particular challenges Russia has faced in wielding cyber power when events on the ground drive rapid changes in operational requirements.

Phase 1: Active Preparation (March 2021–23 February 2022)

This phase began in March 2021 when Russian cyber groups increased efforts to pre-position and secure persistent access to Ukrainian critical infrastructure.[7] Notably, this increase in cyber activity occurred at the same time as Russia's initial massing of forces around Ukraine's borders that raised concerns of a potential invasion. However, unlike the broader military build-up, these cyber operations were not a complete change in course for the controlling units, but instead an intensification of long-running operations by Russia's intelligence services against Ukrainian critical infrastructure networks. To illustrate, months before the invasion, the cyber unit within the Russian military-intelligence force, the GRU, reportedly reactivated dormant intrusions dating from as far back as 2019. These were then used to pursue OCO objectives on invasion day.[8] From what is publicly known, rather than turning to sensitive 'breakglass' capabilities as many expected, Russian cyber units overwhelmingly used simple but reliable tactics such as credential harvesting, brute-force techniques and known vulnerability exploitation to gain access to Ukrainian networks.

The active-preparation phase also saw the first limited efforts by GRU hackers to sabotage Ukrainian CII using the *WhisperGate* wiper. Based on the timing of the *WhisperGate* attack (after failed January 2022 Russia–US talks in Geneva and the NATO Russia Council in Brussels during the same month) and the content depicted on defaced Ukrainian government websites, the operation was probably part of Russia's broader psychological subversion efforts against the Ukrainian public leading up to the war. As a desired secondary effect, *WhisperGate* also likely helped to exhaust cyber defenders before the more concentrated cyber campaign planned to begin the invasion. In retrospect, however, this operation was probably a miscalculation by GRU as it wasted valuable network access and provided a wake-up call to global cyber defenders over a month before the invasion.[9] It is worth noting that Russia's invasion was modelled on the assumption it could quickly achieve objectives prior to international support having a material effect on the invasion's outcome. On the cyber front, this preliminary shaping operation seemed to have the opposite effect.

Phase 2: Opening Phase of Invasion (24 February–April 2022)

The swell of preparatory activity from Phase 1 was largely exploited in support of Russia's opening

campaign to quickly seize Kyiv and overthrow Ukraine's democratically elected government. OCOs were used to disrupt fundamental elements of Ukrainian society as part of a long-standing campaign to portray Ukraine as a failed state unable to recover or maintain continuity of essential services.

As the invasion began, Russia aggressively used pre-positioned access to Ukrainian networks to facilitate attacks against a range of CII, strictly focusing on high-priority strategic targets inside Ukraine. This opening barrage saw Russia frontload its more advanced destructive cyber tools such as *HermeticWiper* and *AcidRain* to disrupt command and control (C2) infrastructure, diffuse Ukraine's will to resist and set conditions for the success of Russia's invasion force. The density of operations in the war's early days conformed with the Russian emphasis on cyber disruptions as a precursor to combat operations and the long-theorised incentives for leveraging pre-positioned cyber capabilities early in a conflict.

From the information available, Russia's opening campaign was primarily oriented toward counter-value targets to systematically disrupt the Ukrainian government's ability to function and communicate with the public, and to undermine a wide range of critical infrastructure functions in civilian population centres. For instance, *HermeticWiper* targeted dozens of organisations across an extremely wide spectrum of Ukraine's critical infrastructure providers that included government, aviation, IT, energy, defence industry, agriculture and financial services.[10] Russia also used less potent cyber tools such as *IsaacWiper*, *CaddyWiper* and *DoubleZero* to disrupt critical infrastructure networks in government, financial services and media organisations.[11] Russia aggressively re-used its destructive cyber tools through the opening phase to support the demands for network attacks at scale. This stood in stark contrast to its use of destructive cyber tools prior to the 2022 invasion, where they were limited to one-off attacks on Ukrainian critical infrastructure.

Of those network attacks publicly reported, only the use of *AcidRain* – the wiper responsible for the disruption of satellite modems used by the *Viasat* network on the opening day of the war – was linked to counterforce targeting of vital communications infrastructure used by Ukraine's military.[12] This is perhaps one of the most misunderstood aspects of Russia's cyber campaign. The default presumption is that all network attack activity is intended to produce counterforce outcomes against targets of military value. However, there is a great danger in projecting Russia's conduct based on Western assumptions. Russia's information-confrontation doctrine places a significant, somewhat pathological, emphasis on the psychological potential of its cyber capabilities. The doctrine perceives the value of technical capabilities primarily in their ability to coerce, subvert or otherwise accumulate psychological pressure against its opponent's centres of gravity. Available evidence suggests that Russia pursued during this phase of the war a cumulative strategy in line with this doctrinal view, generating widespread simultaneous and localised disruptions against civilian information infrastructure primarily in parallel with, rather than being interdependent on, its conventional military operations.[13] Russia has undoubtedly carried out other counterforce OCOs, but they have been necessarily concealed from public view by Ukraine's strict operational security protocols.

Despite an almost year-long preparatory phase, there were signs that Russia struggled to sustain the envisioned density of operations beyond the first week of the war. Once the ill-conceived plan to rapidly seize Kyiv stalled and Russia was forced to revise its war plans, reported network attack activity paused for an extended period. Judging from the high volume of frontloaded operations, Russian cyber units may have suffered from a rapid attrition of access to Ukrainian targets, and this undermined Moscow's ability to generate a blanketing of effects beyond the opening salvo. After this pause, Russia's OCOs took on a more scattershot approach. Operations became more tactical and opportunistic, with planners and operators likely forced into action without the time required to properly flesh out newly gained access to Ukrainian networks.

While it is generally true that regaining access to relevant strategic networks would challenge any cyber programme shifting towards a wartime OCO footing, the hurdle was likely particularly large for Russia given the rate at which it depleted its stockpiled access to accumulate early disruptions. Even without the self-inflicted attrition, the degree of difficulty in developing new access to strategically relevant targets under compressed

timelines and a rapidly changing operational environment cannot be overstated. Also, contingencies Russia may have prepared for were almost certainly in part degraded by the extended defensive actions of Ukraine and its partners from late 2021 till early 2022.[14] Factoring in these issues, there seemed to be a significant disconnect between the GRU's envisioned strategy in Phase 1 and its ability to execute it.

Phase 3: Donbas Offensive (April–July 2022)

After Russia's failure to achieve total victory in its initial invasion and the Kremlin's decision to narrow its focus to eastern Ukraine, reported destructive cyber operations against Ukraine's CII significantly decreased. This is not to say that no meaningful activity occurred, but that Russia may not have had the same operational incentives nor the ability to conduct OCOs at the levels of intensity as in the opening phase. Nevertheless, Russia again frontloaded its most advanced cyber capabilities in an attempt to create a more permissive environment for the upcoming Donbas offensive. As Russian forces shifted their gaze from Kyiv towards Ukraine's east, GRU hackers attempted to cause regional power outages by using *Industroyer2*, a modern successor to the malware used to interrupt Ukraine's flow of electricity in 2016.[15]

It is currently unclear why there were fewer cyber disruptions during this phase of the war. One possibility is that the perceived utility of cyber disruptions declined as the war narrowed in on Ukraine's east and became more attritional. According to this logic, Russia's military could have decided that its cyber forces were better suited to focus on presence-based operations away from the front lines in Eastern Ukraine to either gather intelligence or pre-position on infrastructure involved in the sustainment of the Ukrainian Armed Forces. With no quick victory in sight, there was possibly a growing preference for access over action.

It is also possible that attrition from the aggressive tempo of the earlier phase severely impacted Russian cyber forces' ability to sustain operations. Documented efforts to regain access to Ukrainian targets suggest that Russia may not have possessed sufficient access to targets during the transition to the second phase of the invasion.[16] This line of reasoning is consistent with Moscow's delusions about an easy victory and its lack of planning for a protracted conflict. However, recent reporting on *CaddyWiper* operations throughout May 2022 begs the question of whether there were more cyber operations that have yet to come to light.[17]

Irrespective of the volume of OCOs in this phase of the war, the relative increase in novel access operations outside of Ukraine revealed a change in Russia's long-term strategy. Western cyber-security companies outed efforts by Russian cyber groups to gain new access to targets in Eastern European countries during this phase, indicating a broadening of focus beyond Ukraine. For instance, Russia gained in mid-May 2022 the initial footholds in Ukrainian and Polish transportation and logistics networks that *Prestige* ransomware operations later disrupted in early October.[18] Russian cyber groups were also identified conducting access operations against defence and cyber-security organisations in the Baltics during this period.[19] Western officials have likewise detailed Russian efforts to target surveillance cameras likely to inform troop movements and the transit of Western military aid.[20]

In summary, there appears to be an adaptation of priorities and a more expansive set of access requirements on display during this phase of the war than in earlier periods. Based on these publicly known operations, Russia continued to rely on simple but effective tactics such as phishing campaigns, stealing cookies from browsers as well as the exploitation of known vulnerabilities in internet-facing applications and services. Take for example GRU hackers' rapid adoption of the recently disclosed *Follina* vulnerability in June 2022 to lure targets with a repurposed Atlantic Council article on Russia's potential use of nuclear weapons.[21]

But even with the consistency in tactics, a notable change occurred in Russia's malware arsenal. GRU cyber operations factored in an increasing volume of low-equity and intermediary tooling, including an increase in malware from open sources and criminal marketplaces to supplement Russia's custom-made tools. From a wartime-planning perspective, ready-made capabilities available in underground marketplaces are an enduring concern as they allow state actors under resource or time pressures to rapidly generate capabilities for new offensive operations.[22]

Considering the efforts to diversify its malware arsenal, it is reasonable to assume that Russia also sought to supplement its own access operations against critical infrastructure targets with capabilities from criminal marketplaces where possible.

While Russia's overall arsenal broadened, its destructive arsenal significantly narrowed, with *CaddyWiper* emerging as the favourite from at least a dozen unique malware variants used in the opening campaign of the war. What accounted for this development is not clear at present, but there has been a distinct effort to extend the longevity and advance the offensive potential of this specific wiper in comparison with the others that saw frequent use in February and March 2022. Whatever the underlying reasons, this development highlights the GRU's capacity for adaptive learning to cope with the challenges of an unexpectedly prolonged conflict.

Phase 4: Ukraine's Counter-offensive (August–November 2022)

With details of Russian OCOs during Ukraine's counter-offensive still emerging as this paper was written, it is premature to comprehensively assess the changing nature of Russian OCOs in this phase of the war. Nevertheless, there were early signs that Russia continued to adapt its operations to overcome the earlier difficulties it faced in balancing access and action. Russian cyber units continued to diversify methods for gaining access to Ukraine's CII[23]. They also deepened their long-standing preference for commodity tools to backfill their arsenals more rapidly than if solely relying on internal development resources.[24]

An uptick in reported network attacks starting in October 2022 revealed a more prepared and reinvigorated cyber programme compared with that of summer. Notably, increased Russian network attacks against energy, water and logistics organisations beginning in October coincided with systematic targeting of Ukraine's energy infrastructure using missiles and loitering munitions. This pointed to a coordinated strategy to ratchet up cross-domain pressure and deprive civilians of critical services as winter approached.[25] Russian services also conducted reconnaissance against natural gas targets in other parts of Europe, an area of likely acute interest given the energy-security dynamics surrounding the war.[26] This continued expansion of interest in critical information networks outside of Ukraine underscored the warnings from the Finnish Security and Intelligence Service of a more assertive and integrated use of cyber operations as the war continued.[27]

Chapter Two: Takeaways from Russia's Cyber Offensive

Balancing Access and Action

There are several key takeaways from Russia's evolving cyber campaign that can aid our understanding of Ukraine's defence. The first is that offensive cyber operations in practice are likely to be cyclical by nature. As we can see from Russia's efforts to replenish access to critical infrastructure networks throughout the first year of the war, gaps in offensive network action should not be interpreted as the consequence of cyber groups letting up or exhausting their operational capacity. Rather, there had been a continuous effort to probe critical infrastructure, build contingency access methods and diversify tools and tactics to prolong Russia's ability to conduct OCOs. New operational cycles have also come with adjustments in priority that have rapidly placed new technologies, suppliers and organisations at risk. Defenders preparing for future waves of Russia's cyber campaign must recognise that there will be a continuous need to re-target, re-tool and re-establish access when priority is being given to a disruptive mandate. And with newly discovered vulnerabilities being frequently discovered, the adversary will find opportunities to bypass defences. It is therefore crucial to invest in a layered defensive posture that can sustain attack surface reduction, network detection and basic cyber-hygiene practices on top of the increased resource strain likely to be forced onto incident-response functions. Overcoming attrition of access will be a paramount concern for any offensive programme in a wartime environment.

Russia's Information Confrontation Doctrine and Cumulative Strategy

The second lesson relates to targeting. Russia ostensibly pursued a cumulative strategy with its OCOs, likely perceiving that the minute accumulation of simultaneous disruptions to Ukraine's CII would create a critical mass beneficial to Moscow's war aims. This component of Russia's strategy had likely not focused on targets of military value, but on strategic targets that would impact the morale of Ukrainian leadership and civilians – centres of gravity in its broader coercive strategy to erode Ukraine's will. Russian targeting had therefore been much more widespread and indiscriminate than pre-war estimates envisioned, with CII valued by Moscow not solely in terms of its military utility, but primarily in its potential to disrupt civilian infrastructure and compound other means of societal-wide psychological pressure. It is important to avoid falling into the trap of seeing cyber operations as a substitute for kinetic firepower and instead consider their potential remit in pursuing broader strategic wartime objectives beyond the battlefield.

Russia's targeting patterns also point to a critical flaw in its overall cyber campaign – the incongruence between its concept and conduct of operations. All three of Russia's intelligence services possess highly capable cyber elements. The Federal Security Service is known to possess a destructive cyber programme similar to the GRU.[28] Yet from what is publicly known, only the GRU conducted OCOs against Ukrainian critical infrastructure. What accounts for this limited use of existing operational capacity remains unclear. Perhaps institutional inertia resulted in adherence to Russia's historical rules of engagement for destructive operations, with the Russian military's cyber-sabotage teams commonly known as *Sandworm* continuing to take the lead in wartime. Alternatively, Moscow may have perceived that task specialisation – with specific units focusing on initial access and others on sabotage – would have enabled a more scaled and holistic use of its military cyber programme. Nevertheless, beyond the armed forces, one would expect a wider involvement of Russia's other services. The apparent cumulative strategy that Russia opened the war with would have logically benefited from additional manpower and resources for OCOs. The erroneous assumptions that underpinned Russia's short-war thinking and its renowned inter-service rivalries likely impeded better integration at the operational level.

Operational Pressures in a Contested Environment

The third takeaway relates to sustaining operations in a contested wartime environment. While predictions often model the use of highly sensitive capabilities carefully husbanded for conflict, Russia overwhelmingly opted for a more generic concept of operations. Russian cyber units doubled down on their long-term interest in targeting the perimeter of target networks by focusing on 'edge' devices such as routers, firewalls and email servers that can be exploited using known vulnerabilities for immediate access.[29] This approach is advantageous as it can be harder to detect, can defeat 'impossible travel' and other geographically rooted defensive measures, and does not leave trackable artefacts from purchasing C2 infrastructure.[30] And because incidents involving edge devices such as routers are not often remediated during incident response, they at times provided Russia's military persistent access in order to re-strike networks at a later date. Notably, reports from threat-intelligence firms continue to highlight network infrastructure as a significant blind spot for defenders in large part due to visibility limitations imposed by network suppliers.[31] This is an area that warrants much more defensive attention.

Similarly, Russia opted for more simple and light-weight destructive cyber tools than it historically used for OCOs, shifting to an arsenal that is easier to operate across a wide range of targets and with more predictable and consistent outcomes. Judging by the common design across most of the destructive malware in Russia's arsenal, there seems to be a recognition that to achieve faster, more immediate effects, there is a benefit to tooling that is intuitive and can capitalise on pre-existing programmes and processes native to the victim environment. Moreover, by possessing field-ready malware that forego the need for lengthy reconnaissance and tailoring cycles, Russian cyber units have likely enabled a greater range of non-expert operators to be on the offensive, increasing their overall capacity to conduct cyber operations. Take for instance the reported operations launched from offices seized by Russian troops against connected networks in Ukrainian-held territory.[32] Simple and intuitive tools are helpful to enable such wider participation.

It can be tempting to view the generic and opportunistic nature of Russia's cyber tactics and tools as being astrategic. But such judgments misunderstand the structural incentives that underlie exploitation at scale, particularly in a contested environment. Access restores mobility for cyber forces and enables action. It is therefore characteristically beneficial for cyber programmes to keep operational complexity to a minimum and attempt to achieve economies of scale when gathering access to relevant targets. Looking toward the future, similar tradecraft preferences will likely factor into other crises and conflict scenarios where there would be demands to support a higher than usual operating tempo.

Chapter Three: Ukraine's Cyber Defence

While a definitive picture of Russian OCOs has not been provided thus far, the weight of evidence from the first year of the war indicates that Ukraine has absorbed a concerted and intense campaign of network attack activity and supporting access operations. Without strong and effective cyber defences, the impact of Russia's cyber campaign on Ukraine could have been much worse.

At this juncture, it is important to stress that the lion's share of credit for defensive success lies with Ukraine. International partnerships with Western governments and private-sector technology firms have undoubtedly made significant contributions to Ukraine's capabilities.[33] But it is Ukraine's preparation, pragmatism and long-term commitments to improving its cyber defences and resilience that have made the difference. Years of investment and experience dealing with unparalleled levels of cyber aggression have provided the necessary baseline capabilities to integrate national efforts with diverse forms of external support. Kyiv's capacity for success was engineered well in advance of the February 2022 invasion.

Instead of focusing on Ukraine's long-term adaptations, which have been covered extensively elsewhere, this analysis will narrow in on Ukraine's shorter-term actions after March 2021 and the initiation of Russia's preparatory phase. Similar to Russia's offensive, we must keep in mind that many of Ukraine's defensive actions are classified, as the war is ongoing. As such, what follows is not a comprehensive analysis, but a preliminary look at some of the key factors identified to date that may inform the adaptations under way in other national, multinational or private cyber-defence structures.

Phase 1: Active Preparation (March 2021–23 February 2022)

Currently, there is limited public visibility into the defensive actions Ukraine's national cyber authorities took during the year-long active preparation phase. Yet given what we know about Kyiv's ability to absorb and bounce back from Russia's cyber offensive, there were clear signs during this phase that Ukraine had made strides in implementing the national cybersecurity system envisioned in its 2016 national cyber-security strategy.

At a more granular level, we can loosely estimate what contributed to Ukraine's success based on the characteristics of Russia's preparatory phase. Russia's reliance on common tactics for pre-positioning in CII networks, such as spear phishing, credential harvesting and exploiting known vulnerabilities, meant that Ukraine's ability to carry out basic protection measures at scale and with consistency was likely foundational to its success. In practice, this likely entailed the aggressive pursuit of best practices such as closing visibility gaps with cyber-observable data; hardening remote entry points into CII networks; supplementing passwords with multi-factor authentication; adherence to the principle of least privilege for administrative and service accounts; and threat hunting to detect instances of long-term access gained through legitimate compromise credentials.

Efforts to raise the bar for initial access also necessarily included rapid application of security patches and conducting assessments to proactively identify known vulnerabilities prior to their opportunistic exploitation by Russian cyber units. On the resilience side of the coin, emphasis placed on the physical and digital migration of equipment and backups to more secure locations showed Ukraine's pragmatic recognition that certain network attacks will succeed and that loss of a network need not result in permanent loss of vital systems and data.[34] Similar investments also likely paid off for Ukraine's more sensitive networks. The fact that *Industroyer2* was detected and neutralised shortly after its use would suggest that Kyiv had taken steps to increase its visibility and monitoring of critical industrial assets and the external connections to its OT network environments. While this is just one example from one of Ukraine's regional power distribution

entities, Ukraine's national efforts to harden CII against network attacks in response to the energy-grid disruptions of 2015 and 2016 have almost certainly permeated other critical infrastructure sectors in the country.

It is also important to consider Ukraine's non-technical adaptations that have helped improve its cyber defences. In this regard, examining the country's national cyber authorities and its operating model would be instructive. In May 2021, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) opened the UA30 Cyber Center, a heavily promoted re-launch of the State Cyber Protection Centre which centrally houses the national response teams and security operations centre and provides a focal point for national cyber-defence efforts. Notably, the SSSCIP has civilian and military responsibilities, and this dual function has had mixed reviews due to the potential complications for building trust and engaging with private industry.[35] However, the the service's civil-military integration has probably provided Ukraine with an invaluable common operational picture under one roof, including centralised visibility and economies of scales for protecting military and non-military public and private CII. In accordance with Ukraine's cyber-security strategy, the SSSCIP maintains a national register of CII assets within Ukraine and has established points of contact to compile updates of their cyber-defence requirements. This unified command structure has also very likely enabled Ukraine to streamline engagement with the relevant public- and private-sector actors.

The period before the invasion was also when Ukraine began to ramp up its outreach to other governments and the private sector. Starting in December 2021 as the likelihood of invasion increased, Ukrainian cyber personnel hosted their counterparts from US Cyber Command to hunt for evidence of Russian cyber units pre-positioning themselves in critical infrastructure networks. American cyber forces also provided support beyond direct countermeasures, such as remote analytic and advisory support to enhance the resilience of priority networks.[36] This joint operation reportedly led to the removal of pre-positioned destructive malware in Ukrainian Railways networks prior to the invasion, preserving the ability of Ukrainians to escape to safety when the war started.[37] Results of the hunt-forward mission were then shared with government partners and the private sector to scale out global cyber defences and visibility into similar activity.[38] Given the length and scope of the engagement with US cyber forces, as well as reported similar support from the UK and others, it is almost certain that these hunt-forward operations were able to evict further instances of Russian pre-positioned access and malware.[39] While it is difficult to measure the exact impact of this external support, the use of outside parties to supplement national cyber defenders was likely highly consequential in seizing initiative away from Russia's cyber units and in preventing overextension of Ukrainian personnel given their extended high tempo of defensive operations.

Legislative reforms during the preparatory phase were also a crucial enabler for Ukraine's long-term success. On 17 February 2022, a week before the invasion, Ukraine's parliament approved legislation to allow public and private CII to migrate into cloud infrastructure abroad.[40] These measures were later enhanced under martial law.[41] This allowed Ukraine to back up and safeguard vital state registers and databases with key cloud service providers. It also paved the way for emergency migration of critical services to European data centres outside the reach of conventional attacks, such as the reported missile strikes against Ukraine's government data centres.[42] Ukrainian officials have been vocal in acknowledging the impact that the cloud migration has had on the continuity of core government services and the functioning of the economy, claiming that 'not a single registry has stopped operating' as a result of Russia's cyber offensive.[43] In the year-end meeting of Ukraine's National Cyber Security Cluster, officials highlighted the crucial role that legislative amendments played to enable CII protection and other aspects of Ukraine's defensive posture.[44] A full analysis of these legislative changes is beyond the scope of this paper, but it is surely deserving of further policymaker attention.

Phases 2–4: Opening Phase of Invasion, Donbas Offensive and Ukrainian Counter-offensive (24 February–November 2022)

After Russia invaded, the core defensive principles outlined above constituted the bedrock of Ukraine's cyber defence, but there were specific elements that occurred after invasion day that warrant more detailed attention.

First and foremost, Ukraine had specific contingencies in place for a Russian invasion. On 24 February 2022, Ukrainian incident-response teams (which were mainly based in and around Kyiv) reportedly executed plans to disperse across the country to reinforce regional-response offices in expectation of large-scale network attacks.[45] As Ukraine is one of the largest countries in Europe, this diffusion of responders was instrumental in enabling a more rapid response to Russia's extremely broad targeting of critical information infrastructure. This move spared response teams the need to make long and potentially hazardous journeys from the capital region to victims of network attacks in other parts of Ukraine. This helped Ukraine rapidly triage victims, prioritise analytical resources and speed up incident response or other forms of risk mitigation. To implement this strategy, it would also mean that Ukraine had acquired additional expeditionary incident-response kits – equipment to conduct vulnerability analysis, incident response and other cyber-analytic functions – prior to the war to support its planned decentralised response.

Immediately after the invasion, Ukraine also began to elicit support from the private sector to supplement its own cyber capabilities. One aspect of this effort was to call on national private-sector experts. Requests for volunteers to help protect CII were reportedly circulated through communities at the request of a senior Ukrainian defence ministry official. These volunteers were requested to help defend infrastructure, identify critical vulnerabilities and carry out other defensive tasks.[46] Even as an ad-hoc initiative in response to the invasion, this pool of resources gave Ukraine invaluable 'bench depth' to manage Russia's cyber operations. Another measure was fostering cyber partnerships with international firms. Cooperation with the likes of Microsoft, ESET, Google and others added defensive depth to Ukraine's CII. The move also provided Ukraine's cyber defences with expert personnel on top of cutting-edge detection and response capabilities. This extended ecosystem of support provided unprecedented visibility into emerging threats and, on multiple occasions, early warning to prevent successful network attacks from reaching their full potential. Most notably, on at least two occasions – a destructive malware targeting a shipping company in Lviv and the *Industroyer2* operation against Ukraine's energy infrastructure at the onset of the Donbas offensive – Ukraine proactively disrupted Russian operations through coordinated detection and response with these international, non-governmental partners.

This swell of private-sector support occurred against the backdrop of continued cloud migrations, as well as intelligence sharing, remote analytic support and network defence activities coordinated with other governments. The key takeaway here is that even with highly capable and experienced cyber defenders, no existing national cyber programme is adequately resourced to withstand a prolonged and intensive cyber campaign as shown in the Ukraine war. The ability to tap into the surge capacity and unique strengths of government agencies and the private sector has been key in countering Russia's increasing cyber exploitation. Ukraine's orchestration of support from international partners also underscores the operational reality that no single entity has uniform visibility into the campaigns, capabilities and infrastructure of Russian threat groups. Data sharing collaboration with partners possessing distinct telemetry and analytic capabilities has provided Ukraine with the ability to produce a comprehensive common operational picture of Russian OCOs and keep pace with the way these operations have evolved throughout the war.

Early measures were also taken to cement Ukrainian advantages in the information environment and reduce the network attack surface for exploitation originating from Russian internet and mobile networks.[47] In the war's first week, Ukrainian regulators made the decision to block internet traffic from hundreds of autonomous systems that formed the backbone of the Russian internet.[48] Ukrainian authorities also made similar mobile network-security decisions in early March 2022, such as implementing national emergency roaming across carriers and suspending all inbound roaming, phone calls and SMS from Russia and Belarus.

Another factor for Ukraine's cyber-defensive success was its tight operational security. Ukraine's national cyber authorities had demonstrated a careful and purposive approach to sharing information about Russian cyber operations without revealing sensitive details about their impact. The prudence of this strategy lies in the particular difficulties of conducting battle damage

assessments in cyberspace.[49] Network attacks rarely leave physical traces, meaning that even if an OCO is successful, there is no reliable verification method for confirming the effects of the attack. In many cases, the successful disruption of a network will also eliminate the access of the adversary, denying it a crucial source of information for determining whether the desired impact is achieved. And even when there can be some certainty that the network attack has been a success, it is difficult to interpret the longevity of the effects and whether they were able to bring about the intended second-order consequences to the target. For these reasons, the victims of OCOs can be crucial forms of feedback to the adversary.

Ukraine effectively denied Russia this feedback channel. Beyond the *Viasat* disruption which had visible cascading effects in neighbouring European countries and forced a public acknowledgment of the operation, Ukrainian national cyber authorities have not publicly disclosed any counterforce network attacks that directly impacted military systems or networks. In instances where Ukraine shared details of Russian cyber operations against civilian targets, the information was limited to network defence intelligence about the tools and tactics used and excluded specifics regarding the impacted organisation, the downtime experienced or other aspects of the impact. Ukraine has struck a careful balance in what it shared publicly, helping to increase global visibility into Russian cyber groups and to build collective defences against similar activity. This helped to deny Russia the desired second-order psychological effects from its operations. Attempts by Russian-aligned information operations on Telegram to solicit media coverage and provoke a public response to Russian OCOs have been unsuccessful to date.[50]

Chapter Four: Takeaways from Ukraine's Cyber Defence

Early and Active Contestation

The central lesson to be drawn from the Ukrainian cyber effort is that the defence gets a vote. Russia's planned cyber offensive was significantly undercut by early and proactive defensive actions by Ukraine and its network of partners. These efforts have continued to the present, constraining the potential scale and potency of the impacts Russia has been able to achieve against Ukraine's CII. Even in instances where Russia successfully disrupted networks, destroyed data or denied access to vital government services, Ukraine's preparation, agility and determination seemingly rendered their impacts short lived.

There is an unavoidable truth underlying competition and conflict in cyberspace that network attacks will inevitably succeed. Russia's offensive units have found ways to disrupt networks despite an unprecedented coalition of governments and private firms with global visibility bearing down on their campaigns, tools and infrastructure. However, these glimpses of success have been hard earned. Defensive friction has seemingly forced Russian cyber units into adopting simpler and more opportunistic tools and tactics more than likely desired. Decreasing OCOs after the opening invasion phase likewise indicate that Russia has struggled to sustain effective offensive output and has been limited to a more measured pace of activity in the subsequent months. Proactive defensive interventions have helped to seize the initiative from Russia and contest their planned courses of action.

However, others seeking to replicate Ukraine's model of success should recognise that building an effective cyber-defence posture is a marathon, not a sprint. Ukraine's capacity to withstand Russia's offensive stems from incremental improvements in its cyber defences over years of painstaking effort and investment. The specific plans and contingencies developed for the war would not have been possible without modernising national cyber-defence systems and raising the maturity levels of public and private critical infrastructure providers in the years leading up to the invasion. Take for example the unprecedented levels of threat intelligence sharing from external partners – undeniably a significant boon to Ukrainian situational awareness and ability to detect emerging threats. Without prior efforts to close visibility gaps, train defenders and adopt a more active cyber-defence posture, the ability to integrate and exploit this intelligence at scale would have been severely limited. Ultimately, early defensive actions can undermine the adversary's planning and intentions, but sound fundamentals are required to sustain those advantages.

The Importance of Institutional Adaptation

Ukraine's defence has not been faultless or omnipotent. As the aphorism goes: 'No plan survives first contact with the adversary'. It is impossible to anticipate every eventuality, particularly in a domain as fluid as cyberspace. Ukraine's national cyber authorities have undoubtedly been forced to make difficult decisions around which critical infrastructure networks to prioritise for response, particularly with Russia's mass-based and at times opportunistic approach to OCOs. It is reasonable to presume that Kyiv has tolerated some degree of network loss to manage the extreme demands placed on its regionally distributed incident-response teams. Yet much like in other aspects of the Ukrainian defence of its country, what has made the difference is its extraordinary capacity for institutional adaptation.[51]

Absorbing External Support

Through iterative learning, Ukraine has transformed its national cyber-defence system to absorb diverse forms of external funding and support. It has rapidly forged cooperative architectures to absorb volunteer defenders, migrate data and services to the cloud and to consolidate different forms of technical assistance. The result? Defensive reach far beyond what it could have achieved alone. Indeed, the Ukrainian experience underscores the importance of building partnerships with a range of

national private-sector actors and international partners to increase capacity for intervention and to maintain visibility into the adversary's emerging courses of action. In this regard, the willingness to modify existing legislation and practices is key.

Nevertheless, it is important to recognise that despite the success, these partnerships have largely been improvised. Ukraine has cobbled together an extended ecosystem of defensive support that the SSSCIP has deftly orchestrated and executed. But it will require careful planning, resourcing and institutionalisation to ensure the long-term sustainability of this unified response model through the end of the war and beyond. Take for example the widespread disruption of Starlink communications devices on the frontlines in late September 2022.[52] The outages have raised concerns about the ad hoc nature of private-sector help and the potential pitfalls of relying on the benevolence of private firms for CII provision. Looking forward, tailored strategies will be needed to iron out the kinks in these strategic partnerships. Closer integration of processes and funding to subsidise the private sector's commitments of resources will be crucial steps for more consistent and sustainable results. If anything, Ukraine has shown that there is a lot of untapped potential to be realised.

Moreover, there are opportunities for governments to better share the defensive burden. The Ukrainian experience underscores the importance of quick response and the ability to disperse response capacity across impacted sectors and regions. Yet this will require significant strengthening of existing national capacities. Response functions in most Western countries are built solely (if adequately) to address national demand. And to date, multilateral mechanisms for threat-intelligence exchange and rapid response have been areas of underinvestment – they are largely treated as deterrence messaging rather than well-developed and exercised capabilities. This is an area where dedicated investments could significantly bolster collective defences. Commitments to improving interoperability and enabling virtual incident response would also significantly boost these existing capabilities. These deeper investments in joint capabilities could help to burden share and make a unified response more sustainable for all parties involved. To fully absorb the lessons from Ukraine, reforms should likewise plan for better incorporation of private industry into national and multinational exercises given their frontline role in protecting critical networks.

Expanding to the Cloud

Ukraine's emergency migration to the cloud has conferred immeasurable benefits. Within days of the war breaking out, key CII assets and services came under the protection of Western technology companies, allowing Ukrainian authorities to maintain access and control over vital state functions. The uptime afforded by the public cloud cut across various critical services. Banking systems kept working, trains kept running on schedule, and Ukraine's military kept its vital connections to situational awareness data.[53] Physical risks to data centres and incident-response personnel were likewise mitigated. It is without a doubt that all future wartime plans would benefit from relocating CII assets to safer areas to maximise their resilience.

That said, current policy debates are placing far more weight on emergency cloud migrations as part of future wartime responses than is helpful. Rapid migrations like the ones enabled by companies such as Amazon Web Services, Microsoft and VMWare often require specialised technologies and physical access – both of which may not be readily available in the short-term horizon of a crisis. It would therefore be wrong for others to conclude they can pull off an emergency migration the same way Ukraine did. Planning for such eventualities should ideally be well in advance and supplemented by other measures.

The cloud is also not a defensive panacea. Migrations of existing data and services will often require carrying over existing (legacy) technologies and processes which may remain vulnerable to exploitation. Moreover, the defence of these hybrid network environments can be much more complex, with links with on-premise assets providing potentially novel pathways leading to compromised connected cloud environments. Paradoxically, while the cloud may mitigate other categories of risk, it leaves cyber operations as the only means of meaningful exploitation and denial at the adversary's disposal. Cloud environments are therefore likely to rapidly become targets of new cyber operations, extending the overall attack surface that requires protection. Organisations seeking to incorporate the public cloud will therefore have to familiarise

themselves with cloud-specific data sources for threat intelligence and the unique method used by adversaries in these environments to ensure baseline levels of protection can be implemented.

Maintaining the Initiative

The final lesson is a word of warning: We should not let Ukraine's success engender a false sense of security about OCOs in future conflicts. As established, Kyiv's defensive achievements thus far are not preordained. Likewise, Russia's inability to achieve more lasting cyber disruptions is not due to the inherent advantage the defending side has in cyberspace, nor is it proof that network attacks hold no strategic potential. On the contrary, we have seen meaningful impacts from Russia's cyber operations and of its various near misses that held the potential to affect the early contours of the war. All these occurred despite the glaring issues that challenged Russia's ability to employ its highly capable cyber forces to their maximum potential.

Caution is therefore required not to overinterpret Russia's underperformance relative to Ukraine's defence. The reality is that the war is not over. Interactions between offence and defence could still change as Russia continues to learn from its early shortcomings. And from what was seen from Russia's cyber forces leading into the winter months, persistent efforts to generate cyber disruptions at a national scale will almost certainly continue. The ability to sustain national lines of effort and prop up external support will be highly consequential in the extended success of Ukraine's cyber defences.

Chapter Five: Lessons for a Taiwan Contingency

Many have rightfully observed the cyber dimensions of Russia's war with an eye towards Taiwan. Speculation about Chinese preparations for a potential invasion of the island has increased since Moscow's attack on Ukraine, with the broader parallels between the two situations hard to ignore. Moreover, with the Ukraine war being the first major inter-state conflict involving the large-scale employment of OCOs, there are varied insights to extract from both Russian offensive and Ukrainian defensive performances that may be directly relevant to a Taiwan contingency. It is hence reasonable to assume that both Taipei and Beijing have recognised this reality and are monitoring the conflict to extract relevant lessons.

Insights for a Chinese Offensive

We should not overinterpret Russia's cyber campaign as a model that China should, or is likely to, follow. Russia's opening cyber offensive was a miscalibrated strategy grounded in the search for a quick and decisive victory. Derived from its particular view of OCOs as an instrument of adverse influence, Russia appeared to have believed it could amass psychological pressure in and through cyberspace that would 'disorganise' a coordinated response from Ukraine and reduce its capacity to resist.[54] Russia therefore opted for a frontloaded and intense campaign of wide-ranging simultaneous disruptions against an array of counter-value targets, forgoing more tailored options with the potential for more lasting or cascading consequences. Intensity and scale, however, had not been the guarantors of impact that Russia had envisioned owing to Ukraine's unanticipated defensive reinforcements. Moreover, with the relative focus on counter-value targets resulting from its short-war assumptions, Russia seemingly failed to develop appropriate contingencies against targets of military relevance.

Simply put, it would be a mistake to view cyber operations in Ukraine as paradigmatic for future conflicts. Russia's campaign was far from a showcase of offensive cyber's true warfighting potential. Despite lofty expectations for what is arguably the most experienced offensive cyber force in the world, Russia came up well short of successfully integrating offensive cyber capabilities into its military operations. Moscow's rigid and parochial use of OCOs failed to exploit their wide range of possibilities and unique situational advantages that cyber capabilities can afford during a conflict. And with a few exceptions, Russia seemed not to have pursued any concerted efforts to conduct combined arms operations or to sequentially integrate OCOs directly with its military activities. Whatever the root causes of this failure, they have functionally limited offensive cyber's potential as an operational enabler and force multiplier.

These are not miscalculations China is likely to repeat. Chinese doctrine perceives centres of gravity differently compared with Russia, and Beijing emphasises the broader enabling or constraining effects of cyber operations when used in combination with other strategic military capabilities. People's Liberation Army (PLA) cyber forces – housed within the Strategic Support Force (SSF) – are structurally optimised for joint integrated operations, with their overarching purpose to provide the PLA's senior leadership and theatre military commands with decision advantage and technical-support capabilities such as OCOs. To ensure their readiness for combined-arms operations, SSF elements regularly feature in joint exercises with theatre commands, as well as the navy, air force and rocket forces.[55] Collectively, these efforts to modernise the PLA would suggest a growing competency to integrate cyber operations as part of a combined-arms package.

Consequently, with the PLA's focus on offensive cyber capabilities augmenting conventional force, expect OCOs to feature during the early stages of an invasion (alongside kinetic and electronic-warfare capabilities) to devastate C2, suppress air defences as well as impede enemy air and maritime operations.[56] Compared with Russia's offensive in Ukraine, however, the Chinese campaign would necessarily involve a much heavier concentration of counterforce targeting

in the opening salvo, on top of more concerted efforts to impede communications infrastructure and seize the initiative in the information environment. Depending on the scale of the conflict, the PLA could also seek to leverage OCOs to slow any intervention or international support in support of Taiwan in the way that Russia has been unwilling to do so thus far in Ukraine. Indeed, network attacks with their ambiguity, reach and scale would provide an attractive option for disrupting transportation and logistics CII. In contrast to Russia's cumulative strategy in Ukraine, we could see China using a more calibrated use of pre-positioned access to wider Taiwanese CII networks to preserve contingencies for later stages of an invasion and avoid early attrition of access. [57]

Chinese cyber forces also benefit from several advantages their Russian counterparts do not have. Judging from the volumes of peacetime exploitation linked to Chinese hackers, Beijing holds a substantial manpower advantage for network-reconnaissance and access operations. How this advantage translates into its ability to sustain network attacks remains to be seen, but the PLA likely enjoys a substantial edge in gaining and maintaining access to desired target networks. In addition, Beijing has gone to great lengths to demonstrate the strength and depth of its offensive arsenal. For instance, at national bug-bounty competitions, Chinese researchers have brandished exploits to a range of high-value CII assets likely to be present in sensitive networks.[58] Such signals are a veritable show of force of China's national vulnerability-research ecosystem into which the PLA can likely tap to fuel its OCOs. Considering China's deep national talent pool and regulations mandating the disclosure of vulnerabilities to the government, the PLA is likely better equipped to replenish access and sustain the intensity and duration of its operations. China has also significantly invested in its ability to test and evaluate its offensive cyber capabilities, including through the building of test ranges representative of its potential victims.[59] Not only does this point to extensive reconnaissance of target networks already being carried out, it also shows the maturity of China's offensive cyber programme. Altogether, it seems that China is better positioned and prepared to make use of its cyber forces during wartime than Russia.

The big question mark lies in China's lack of experience. Its cyber forces have not accrued practical experience conducting OCOs during armed conflict. The restructured SSF and its theory of victory remain largely untested in real-world conditions. And despite efforts to alleviate these shortfalls, no amount of investment in test ranges or exercising can replicate the realities of operating in a contested wartime environment or the immense complexity of coordinating OCOs with an invasion force. Even with the benefit of military reforms, more mature doctrine, as well as substantial manpower and capability advantages, it remains to be seen whether the PLA can unlock the force-multiplying potential of OCOs, or they too will underperform in their first real-world operations.

Insights for Taiwanese Cyber Defence

On the defensive side, the lessons from Ukraine are perhaps more durable. The fundamentals undergirding Ukrainian cyber defences can, to some degree, be adopted by Taiwan. In certain areas, these fundamentals can be built upon and enhanced. But replicating this success for Taiwan will require adaptations to China's putative approach to OCOs and the unique geopolitical challenges of a potential Taiwan scenario.

The central lesson from Ukraine for cyber is that the defence has significant control over its degree of vulnerability. Broad-based and sustained investments to implement protection measures consistently at scale, address visibility gaps in critical CII assets and deepen trusted relationships with national critical infrastructure operators are fundamental to adequately understanding and managing cyber risk. Any proactive defence involving similar efforts to actively contest the adversary will require mature fundamentals. As the Ukrainian experience has demonstrated, the ability to quickly respond to successful attacks is equally critical. The Ukrainian model of dispersing incident-response resources to allow for rapid, localised responses across the country is worth replicating. So too is its building of capacity to absorb varied sources of external threat intelligence and analytical support and fuse it with national telemetry. Prioritising defence and response efforts will require comprehensive real-time situational awareness.

Equally central to this success is a commitment to resilience, but this may require novel approaches that factor in geographic realities. For instance, Taiwan can attempt to improve its emergency cloud migration like Ukraine did by dispersing key data assets and services outside of its borders well in advance of any Chinese offensive. Ukraine has provided an invaluable proof of concept that cloud services can enable uptime for critical services when paired with reliable backup communication links such as Starlink – a capability that Taiwan is actively trying to replicate domestically.[60] That said, Beijing's cyber programme has shown the capability to re-route global internet traffic, and it could attempt to hijack internet flows to intercept valuable information flowing to any infrastructure secured in neighbouring countries. China could also attempt to temporarily disrupt the island's outward connectivity to counteract the benefits of any externally hosted critical information infrastructures. Under more escalatory courses of action, China could seek to sever undersea cables that connect Taiwan with the outside world. For Taiwan, the cloud may provide resilience through redundancy, but not necessarily through availability or accessibility in the way it has done so in Ukraine.

Surprisingly, the least translatable aspect from Ukraine may be the defensive support from private companies. On one hand, Taipei can benefit from more forethought and planning on how to integrate external support. In Ukraine, technology and cyber-security firms have been reflexively thrust into their support roles, quickly adapting to the operational realities of the war alongside national cyber defenders. With the benefit of time, external defensive and analytic support can be better orchestrated and integrated into national cyber-defence systems and fill critical coverage gaps. On the other hand, there are multiple risks that warrant careful attention. For instance, China may well focus its OCOs overwhelmingly on sensitive military systems and networks, posing hard security questions on whether to share with private companies the required levels of access to provide their defensive support. From what we can tell, Ukraine has opted to handle the defence of its military networks internally or through the assistance of aligned government agencies, limiting intervention from private-sector partners to defined areas such as government or privately owned CII networks. This allocation of responsibilities has held up well against Russia's broad targeting of civilian infrastructure, but it may not comport with a more surgical, sequential strategy focused on counterforce targets.

It is also not guaranteed that the same few companies that have been indispensable to Ukraine will be willing and capable participants in a Taiwan scenario. The risk calculus behind support for Taipei may not be so clear cut for companies with operations, supply chains or economic interests tied to Chinese markets and production. Moreover, Western technology firms with presence in Europe and familiarity with Russian cyber units may not have the same depth of visibility or experience with Chinese cyber units. Shoring up strategic partnerships with regional cyber-security and technology companies that have extended experience defending against PLA threat groups will be instrumental in any contingency planning. Finally, for more sensitive forms of support such as incident response and data migrations, these firms may not have the same levels of physical access to Taiwanese CII assets due to the island's geography. Even if carefully selected, strategic partnerships with companies inclined to support Taiwan may not provide the same levels of reinforcement from which Ukraine has benefited.

Conclusion

Extracting the enduring lessons from Russia's war in Ukraine – both on the offensive and defensive sides – will surely be at the forefront of policy discussions going forward. As these debates unfold, policymakers need to consider how central Ukraine's superior capacity to adapt and innovate has been to its defensive performance. Moreover, they should recognise that the enablers of this superior adaptive capacity exist largely at the strategic rather than tactical level. Modifications ranging from national legislative changes to strict operational security protocols have combined to negate Russia's advantages and seize the initiative. And throughout the different phases of the war, Ukraine has skilfully adjusted to the nature of Russia's cyber operations and the related political, military and technical challenges. At this juncture, it is uncontroversial to argue that Ukraine has decisively won the adaptation battle in cyberspace.

More importantly, through its defensive actions, Ukraine has shattered the long-held perception of offence dominance in the cyber domain. Kyiv has shown that through preparation, agility and proactive defensive manoeuvres, it is possible to mount a robust cyber defence. Indeed, in a domain as fluid and complex as cyberspace, neither offence or defence is likely to have an inherent advantage.[61] Rather, those who can position themselves to best sense and adjust to a rapidly changing operational environment are most likely to prevail. Key components of Ukraine's defensive model, such as its decentralised response capacity, a well-prepared national cyber defence ecosystem and strong international partnerships, have provided Kyiv this crucial positional advantage relative to Moscow. Reversing the common adage that the enemy gets a vote – equally so does the defender.

But we must also be careful not to read too much into what the Ukraine war means for the general character of cyber warfare. Cyberspace is still a nascent war-fighting domain and Russia's ill-conceived invasion of Ukraine has done little to demonstrate what a well-planned and integrated use of cyber operations could achieve in practice. Moreover, as this paper has established, little remains known about the counterforce applications of cyber operations in Ukraine that are likely to be most consequential to any transferrable military lessons. It is crucial that policymakers acknowledge that the cyber dimensions of any future conflicts, such as a Taiwan contingency, are likely to look fundamentally different than what we have seen in Ukraine.

Notes

1 Jeremy Fleming, 'The head of GCHQ says Vladimir Putin is losing the information war in Ukraine', *The Economist*, 18 August 2022. https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine/.

2 National Cyber Security Centre, 'Lindy Cameron at Chatham House security and defence conference 2022', 28 September 2022. https://www.ncsc.gov.uk/speech/lindy-cameron-chatham-house-security-and-defence-conference-2022/.

3 Alexander Martin, 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', 01 June 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139/; European Commission, 'Joint communication to the European Parliament and the Council: EU policy on cyber defence', 10 November 2022, https://www.eeas.europa.eu/eeas/joint-communication-european-parliament-and-council-eu-policy-cyber-defence_en; and NATO, 'Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy', 10 November 2022, https://www.nato.int/cps/en/natohq/opinions_208925.htm/.

4 See Huib Modderkolk, '*Zo ziet de onzichtbare Russische aanval op Oekraïne eruit*', [This is what the invisible Russian attack on Ukraine looks like], de Volkskrant, 25 February 2022, https://www.volkskrant.nl/nieuws-achtergrond/zo-ziet-de-onzichtbare-russische-aanval-op-oekraine-eruit~baa2304d/.

5 For a discussion on CII, see Dave Clemente, 'Cyber security and global interdependence: what is critical?', Chatham House, February 2013, https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf.

6 Oleksandr Korchenko, Urii Deris and Olga Romanenko, 'Ukrainian critical information infrastructure: terms, sectors, and consequences', National Aviation University of Ukraine, 2017, https://er.nau.edu.ua/handle/NAU/36409/.

7 Microsoft, 'Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine', 27 April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

8 Gabby Roncone and John Wolfram, 'Cyber war on the edge: a balance of access and action', CYBERWARCON '22, 10 November 2022, https://www.cyberwarcon.com/cyber-war-on-the-edge.

9 Tim Starks, 'Did Russia mess up its cyberwar with Ukraine before it even invaded?', *Washington Post*, 4 August 2022, https://www.washingtonpost.com/politics/2022/08/04/did-russia-mess-up-its-cyberwar-with-ukraine-before-it-even-invaded/.

10 Microsoft, 'Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine', and Symantec, 'Ukraine: disk-wiping attacks precede Russian invasion', 24 February 2022, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia/.

11 Alden Wahlstrom *et al*., 'The IO offensive: information operations surrounding the Russian invasion of Ukraine', Mandiant, 25 November 2022, https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.

12 Juan-Andres Guerrero-Saade, 'AcidRain: a modem wiper rains down on Europe', SentinelLabs, 31 March 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

13 Digital Peace Now, Interview with Victor Zhora, 22 June 2022, https://digitalpeacenow.org/stillvulnerable-viktor-zhora/.

14 US Cyber Command, 'Before the invasion: hunt forward operations in Ukraine', 28 November

2022, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/.

15 ESET, 'Industroyer2: Industroyer reloaded', 12 April 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

16 For selected activity, see Computer Emergency Response Team of Ukraine, '*Kiberataka hrupy APT28 z vykorystannyam shkidlyvoyi prohramy CredoMap (CERT-UA#4843)*', [APT28 group cyberattack using the CredoMap malware (CERT-UA#4843)], 20 June 2022, https://cert.gov.ua/article/341128; Computer Emergency Response Team of Ukraine, '*Kiberataka u vidnoshenni operatoriv telekomunikatsiy Ukrayiny z vykorystannyam shkidlyvoyi prohramy DarkCrystal RAT (CERT-UA#4874)*' [Cyberattack against telecommunications operators of Ukraine using the DarkCrystal RAT MALWARE' (CERT-UA#4874)], 24 June 2022, https://cert.gov.ua/article/405538; and Computer Emergency Response Team of Ukraine, '*Ataka hrupy UAC-0056 na derzhavni orhanizatsiyi Ukrayiny z vykorystannyam Cobalt Strike Beacon (CERT-UA#4941)*' [UAC-0056 group attack on state organizations of Ukraine using Cobalt Strike Beacon (CERT-UA#4941)], 11 July 2022, https://cert.gov.ua/article/703548.

17 Roncone and Wolfram, 'Cyber war on the edge: a balance of access and action'.

18 Microsoft, 'New "Prestige" ransomware impacts organizations in Ukraine and Poland', 14 October 2022, https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

19 Billy Leonard, 'Update on cyber activity in Eastern Europe', Google Threat Analysis Group, 03 May 2022, https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/.

20 Maggie Miller, 'Russia's cyberattacks aim to "terrorize" Ukrainians', Politico, 11 January 2023. https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561/.

21 Hossein Jazi and Roberto Santos, 'Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine', MalwareBytes, 13 June 2022, https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine/.

22 JD Work, 'Rapid capabilities generation and prompt effects in offensive cyber operations', SocArXiv Papers, 27 February 2022, https://osf.io/preprints/socarxiv/esx6m/.

23 Mandiant, 'Trojanized Windows 10 operating system installers targeted Ukrainian government', 15 December 2022, https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government/.

24 Recorded Future, 'Russia-Nexus UAC-0113 emulating telecommunication providers in Ukraine', 19 September 2022, https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine/.

25 Clint Watts, 'Preparing for a Russian cyber offensive against Ukraine this winter', Microsoft, 3 December 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

26 Harm Teunis, 'Russian hackers are targeting Dutch gas installations', RTL Z, 25 November 2022, https://www.rtlnieuws.nl/economie/artikel/5348201/hackers-rusland-lng-gasterminal-nederland-europese-unie-cyberoorlog/.

27 Finnish Security and Intelligence Service, 'National security overview 2022', 29 September 2022, https://supo.fi/en/-/national-security-overview-russian-intelligence-changes-approach/.

28 US Cybersecurity & Infrastructure Security Agency, 'Alert (AA22-110A) Russian state-sponsored and criminal cyber threats to critical infrastructure', 9 May 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a/.

29 Andy Greenberg, 'Russia's new cyberwarfare in Ukraine is fast, dirty, and relentless', Wired, 10

November 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

30 For discussion of benefits from targeting edge infrastructure, see Mark Parsons, Judy Ng and Ben Koehl, 'The phantom menace: a tale of Chinese nation state hackers', CYBERWARCON, 10 November 2020, https://www.cyberwarcon.com/the-phantom-menace.

31 Scott Henderson *et al*., 'Suspected Chinese threat actors exploiting FortiOS vulnerability (CVE-2022-42475)', Mandiant, 19 January 2023, https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw/.

32 Amy Mackinnon and Rishi Iyengar, 'Whatever happened to Russia's vaunted cyberoffensive?', Foreign Policy, 16 December 2022, https://foreignpolicy.com/2022/12/16/russia-cyber-offensive-cyberattack-war-ukraine-putin/.

33 Nick Beecroft, 'Evaluating the international support to Ukrainian cyber defense', Carnegie Endowment for International Peace, 3 November 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322/.

34 Raphael Satter and James Pearson, 'Exclusive: Ukraine prepares potential move of sensitive data to another country: official', Reuters, 09 March 2022, https://www.reuters.com/article/ukraine-crisis-tech-contingency-exclusiv-idCAKBN2L62G2/.

35 US Agency for International Development, 'USAID cybersecurity for critical infrastructure in Ukraine. Review of the regulatory framework for critical infrastructure cybersecurity in Ukraine: a legislative assessment report', 22 October 2021, https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf/.

36 US Cyber Command, 'Before the invasion: hunt forward operations in Ukraine', 28 November 2022, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/.

37 Mehul Srivastava, Madhumita Murgia and Hannah Murphy, 'The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion', *Financial Times*, 09 March 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471/.

38 Derek B. Johnson, 'Cyber Command: insights from hunt forward teams in Ukraine flow to US private sector', 05 April 2022, SC Media, https://www.scmagazine.com/analysis/network-security/cyber-command-lessons-from-hunt-forward-teams-in-ukraine-flow-to-us-private-sector/.

39 David Sanger and Julian Barnes, 'U.S. and Britain help Ukraine prepare for potential Russian cyberassault', *New York Times*, 20 December 2021, https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html/.

40 The Law of Ukraine, '*Pro khmarni posluhy'* [About cloud services], 17 February 2022, https://zakon.rada.gov.ua/laws/show/2075-20#Text.

41 Verkhovna Rada of Ukraine, 'Ukraine strengthens its cybersecurity under the martial law', 18 March 2022, https://www.rada.gov.ua/en/news/News/220643.html/.

42 Tim Anderson, 'Russian missiles can't destroy the cloud: Ukraine leader describes emergency migration', The Register, 30 November 2022, https://www.theregister.com/2022/11/30/ukraine_cloud_migration/.

43 Tim Starks, 'Ukraine gets by in cyberspace with a little help from its friends', *Washington Post*, 2 December 2022, https://www.washingtonpost.com/politics/2022/12/02/ukraine-gets-by-cyberspace-with-little-help-its-friends/.

44 State Service of Special Communications and Information Protection of Ukraine, 'National cybersecurity in the context of the war:mMain achievements, plans and prospects', 9 December 2022, https://cip.gov.ua/en/news/nacionalna-kiberbezpeka-v-umovakh-viini-osnovni-dosyagnennya-plani-ta-perspektivi/.

45 *The Economist*, 'Why Russia's cyber-attacks have fallen flat: Ukraine benefited from good preparation and lots of help', 1 December 2022, https://www.economist.com/leaders/2022/12/01/why-russias-cyber-attacks-have-fallen-flat/.

46 Charlie Osborne, 'Report: Ukraine calls for volunteer hackers to protect critical infrastructure', ZDNet, 25 February 2022, https://www.zdnet.com/article/ukraine-calls-for-underground-hackers-to-protect-critical-infrastructure-report/.

47 Cathal Mc Daid. 'The mobile network battlefield in Ukraine – Part 1', AdaptiveMobile Security, 29 March 2022, https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1/.

48 National Commission for the State Regulation of Electronic Communications, Radiofrequency Spectrum and the Provision of Postal Services, '*NKEK prosyt' postachal'nykiv elektronnykh komunikatsiynykh merezh/posluh pospryyaty znyshchennyu informatsiynoyi navaly z boku RF*', [NKEC asks suppliers of electronic communication networks/services to contribute to the destruction of the information invasion by the Russian Federation], 28 February 2022, https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2252&language=uk/.

49 Daniel Moore, 'Offensive cyber operations: understanding intangible warfare (Oxford: Oxford University Press, 2022), p. 95.

50 Mandiant, 'GRU: Rise of the (Telegram) MinIOns', 23 September 2022, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions/.

51 Mick Ryan, 'How Ukraine is winning in the adaptation battle against Russia', Engelsberg Ideas, 24 August 2022, https://engelsbergideas.com/essays/how-ukraine-is-winning-in-the-adaptation-battle-against-russia/.

52 Alex Marquardt, 'Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab', CNN, 14 October 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html/.

53 The New Voice of Ukraine, 'UN recognizes Ukraine's speedy digital migration to the cloud that helped to save industries during war', 28 September 2022, https://english.nv.ua/amp/un-recognizes-ukraine-s-speedy-digital-migration-to-the-cloud-that-helped-to-save-industries-50273248.html/.

54 Michael Kofman *et al*., 'Russian military strategy: core tenets and operational concepts', Center for Naval Analyses, August 2021, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf, pp. 28–29.

55 US Department of Defence, 'Military and security developments involving the People's Republic of China 2022: annual report to Congress', 29 November 2022, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF/, pp. 65, 79, 88; and Department of the Air Force's China Aerospace Studies Institute, 'ITOW: PLA extends "Taiwan encirclement" exercises', 09 August 2022, https://www.airuniversity.af.edu/CASI/Display/Article/3120924/itow-pla-extends-taiwan-encirclement-exercises/.

56 US Department of the Army, 'Chinese Tactics', ATP 7-100.3, August 2021, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf/, pp. 5-3, 7-32–7-34.

57 Moore, 'Asserting Chinese Dominance', p. 186.

58 JD Work, 'China flaunts its offensive cyber power', War on the Rocks, 22 October 2021, https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.

59 Dakota Cary, 'Downrange: a survey of China's cyber ranges', Center for Security and Emerging Technology, September 2022, https://cset.georgetown.edu/publication/downrange-a-survey-of-chinas-cyber-ranges/, p. 1.

60 Kathrin Hille, 'Taiwan plans domestic satellite champion to resist any China attack', *Financial Times*, 6 January 2023, https://www.ft.com/content/07c6e48b-5068-4231-8dcf-fe15cb3d0478/.

61 Michael Fischerkeller, Emily Goldman and Richard Harknett, *Cyber persistence theory: redefining national security in cyberspace* (Oxford: Oxford University Press, 2022), p. 25.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org