CONSIDERATIONS FOR A POST-WAR UKRAINIAN NATIONAL CYBERSECURITY STRATEGY

Thomas JOHANSMEYER*

Abstract

More than three years of war have yielded profound and actionable cybersecurity strategy insight for Ukraine. With the Russian cyber offensive largely disappointing in terms of scale and effectiveness, the enduring lesson for cybersecurity strategists in Ukraine and around the world is that cybersecurity assumptions with regard to cyber war must be revisited. Although the conflict remains ongoing, Ukraine has already begun to think about post-war recovery and reconstruction, an exercise that will include revisiting national security strategy thinking, to include the cyber domain. This article evaluates the impact of the cyber war in Ukraine and what that means for the country's next national cyber security strategy. This article finds that Ukraine should consider three focal points in its next cyber security strategy: (1) the securitisation and prioritisation of the cyber domain relative to the rest of its security strategy, (2) how to balance foreign partnerships with Russia's adversaries to maximise security without provoking its principal adversary, and (3) permitting itself to include the possibility of offensive cyber operations, even if Ukraine chooses not to use that alternative.

Keywords: national security strategy, cyber security, security strategy, cyber war, irregular warfare.

INTRODUCTION

Ukraine published its most recent national security strategy (NSS) in 2020 (National Security Strategy of Ukraine, 2020), and since then, its security

* Thomas Johansmeyer, PhD candidate, Pol&IR, University of Kent, Canterbury. Co-director, Project Instruments of Power, Irregular Warfare Initiative. Early career research member, Institute of Cyber Security for Society (iCSS). ORCID: 0000-0002-3852-5721. Email: trj5@kent.ac.uk

13(1)5-19

environment has changed profoundly. The irregular warfare experienced from 2014, to include a limited occupation and repeated waves of cyber attacks, ultimately led in 2022 to the full-scale invasion the state had long feared. That war has now lasted for more than three years and stubbornly resists the 'mutually hurting stalemate' (Zartman, 2001) that tends to yield the 'ripe moment' (Mitchell, 2008) for peace negotiations. However, the conflict will end at some point, and already, Ukraine has shown it is thinking about post-conflict recovery and reconstruction (Ukraine Government Portal, 2025).

As part of the recovery process, Ukraine will invariably have to produce an updated NSS after the fighting ceases (even if the conflict has not been resolved fully), and with it a refreshed national cyber security strategy (NCSS), the last of which it released in 2021 (National Security and Defense Council of Ukraine, 2021). What the war in Ukraine has already shown is that the next iteration of its NCSS must be nuanced. While support from foreign partners will be crucial to Ukraine's cybersecurity strategy in the future, which the 2021 NCSS included (Johansmeyer, Mott, & Nurse, 2024), there will also be roles and responsibilities specific to Ukraine itself. For a nation accustomed to having to balance its own security needs with the risk of provoking a hostile neighbour, the next suite of NSS materials will likely return to the pre-2022 (and even pre-2014) need to manage the threats it faces from the east while still integrating the lessons it has learned over the past three (and eleven) years.

This article makes a unique contribution to the literature by examining the effects of the ongoing war in Ukraine on the potential direction of the state's first post-conflict cyber security strategy, ultimately providing three important considerations: (1) the securitisation and prioritisation of the cyber domain relative to the rest of its security strategy, (2) how to balance foreign partnerships with Russia's adversaries to maximise security without provoking its principal adversary, and (3) permitting itself to include the possibility of offensive cyber operations, even if Ukraine chooses not to use that alternative. While it may seem early to contemplate what Ukraine's strategy should entail after the war, some lessons are evident already. Further, the conclusions drawn from this process will be of further value to arm's length stakeholders in the conflict (e.g., the United States, United Kingdom, and NATO more broadly) in understanding how they may be called to engage in future cyber security efforts with Ukraine – not to mention for their own security strategy endeavours more directly.

Ukraine likely would not be left to its own devices on security following a cessation of the war, but it also likely will not enjoy full alliance support from NATO and other Western states, at least not anytime in the near term. Within this context, Ukraine's next NCSS should take the 2021 draft's view of the need for international cooperation and collaboration and balance it both with a clearer mission and role for Ukraine itself, based on the lessons from the cyber

conflict and how it interacted with the kinetic war, striking the right balance between cyber security for daily and sub-war exposures while recognising that both civilian and military targets that fail to fall to cyber attacks may be targeted with conventional weapons if the goal is denial of their use.

UKRAINE'S HISTORICAL APPROACH TO CYBERSECURITY STRATEGY

Ukraine's approach to cybersecurity is primarily influenced by the post-Yanukovych period, including the 2014 invasion that led to the occupation of Crimea (Walker, 2023). That period signalled a profound change of direction for Ukraine, attempting to move from the Russian influence (Dickinson, 2024) toward greater engagement with western Europe and the United States, a change Russia saw as detrimental to the local order (Trenin, 2014). The cyber and information portion of this conflict was not the first use of offensive cyber operations by Russia, including in conjunction with kinetic warfare (Mueller et al., 2023). However, it did lead to the treatment of Ukraine as a "testing ground for Russian cyberattacks" since 2014 (Kvartsiana, 2023), having yielded high-profile events such as the 2015 attack against the country's power grid (Johansmeyer, 2024a) and NotPetya in 2017 (Johansmeyer, 2024b).

Ukraine's current approach to cyber security strategy began in earnest in 2021 with its second NCSS. Although the first was published in 2016 (Davydiuk & Potii, 2024), it remained largely neglected until the issuance of the 2021 update, and little of it was implemented (Johansmeyer, Mott, & Nurse, 2024a: 43). The 2021 NCSS draft (Johansmeyer, Mott, & Nurse, 2024a: 48) focused more on the threats the state faced, and ultimately "morphed into an expectation of help from states whose interests would presumably align with those of Ukraine" (Johansmeyer, Mott, & Nurse, 2024a: 43). That is generally what transpired, with western support for Ukraine during the pre-invasion cyber operations of late 2021 and early 2022 mitigating the effects of engagement via the cyber domain and ultimately turning what would only have been of limited effectiveness anyway (Smeets, 2018) into an eventual disappointment (Beecroft, 2022).

The 2021 NCSS draft comes within the context of a 2020 NSS that sees the aspiration of alliance with key NATO members and "shows a greater realisation that the Russian–Ukrainian war will continue" (Kuzio, 2020), to include the prospect of intensification which arose shortly after. According to scholar Andrii Zahorulko, "Currently [in 2020], the main threat to Ukraine remains the use of military force by the Russian Federation; all other threats are derived from it" (Zahorulko, 2020: 684). The statement shows the primacy of military threat over the forms of irregular warfare with which Ukraine had had to contend since

2014, and while the view may not accurately reflect the broad set of security challenges Ukraine faced at the time, it does suggest the ability to manage irregular warfare (including cyber), where a physical invasion would be far more difficult to counter, which clearly turned out to be the case.

Zahorulko's framing provides for the prioritization of strategic threats at a time and in an environment where everything seemed existential (or at least critical). In 2017, the Ukrainian national energy strategy stated clearly that it was developed "against the background of high uncertainty and complications due to the military aggression of the RF [Russian Federation] against Ukraine," which resulted in the "temporary occupation" of Crimea and parts of the Donetsk and Luhansk regions beginning in 2014 (Energy Strategy of Ukraine, 2017: 5). With regard to the cyber domain, Tkachuk (2019a) characterised "the current cyber threats of Russian hybrid aggression" as the backdrop for "the devastating impact of cyber-attacks on Ukraine's critical infrastructure and state information systems that have occurred over recent years" (Tkachuk, 2019b: 2).

The threats, of course, formed only part of the security strategy problem for Ukraine. The other element was the reliability of Western support. The heavy reliance on such support in the 2021 draft NCSS can be seen as a gamble. While US and other western collaboration did come later in the year to help repel the pre-invasion cyber campaign (U.S. Department of State, 2022), the United States' prior track record was indeed inconsistent. The robust support for Ukraine that emerged in the middle of 2021 (Dickinson, 2021) was much more limited in the wake of the 2014 invasion. At the time, the application of the so-called "Obama Doctrine" to Ukraine (Pifer & Herbst, 2016) makes clear that "Ukraine is a core Russian interest but not an American one, so Russia will always be able to maintain escalatory dominance there" (Cordesman, 2016). Russia was dismissed as a regional power (Haddad & Polyakova, 2018), thus relegating the security of Ukraine to a regional issue (Rumer & Sokolsky, 2019). Strategically, Ukraine was caught between two powers (Johansmeyer, Mott, & Nurse, 2024a: 48), one an adversary and the other an occasional and uninterested advocate, at best.

The 2020 NSS thus came against the backdrop of the clear and obvious strategic threats Ukraine faced at the time, a recognition that kinetic war was likely (and realised soon after), and a sense that the support it would get from western states would be limited. Again, the Obama Doctrine was seemingly unequivocal. Therefore, it is easy to conclude that the range of security strategy alternatives available to Ukraine was slim at the time (Johansmeyer, Mott, & Nurse, 2024a: 49). After all, there is little a state can do when several years of irregular warfare from and partial occupation by a larger, more powerful, and immediately adjacent adversary threaten to escalate.

This challenge clearly extends to the cyber domain, where Ukraine saw itself similarly threatened and over-matched. Consequently, the context provided by the NSS for the NCSS is one of aspirational alliance, with a focus on achieving full membership in both NATO and the European Union (Getmanchuk, 2020). Although there has been some indication that Ukraine will be integrated into the broader European community after the conflict, the exact nature of that has yet to be determined. The prospect of economic integration through membership in the EU (European Union, 2024) seems far more realistic than membership in NATO or other mutual defence alliances and arrangements (Rumer, 2025).

The aspiration for alliance in the 2020 NSS and 2021 NCSS represents an evolution in Ukrainian security strategy at the time, relative to earlier strategy publications. Prior to the 2022 invasion, Ukraine saw itself as needing to maintain a balance between the interests of two major powers (Fedoniuk, Karphchuk, & Yuskiv, 2023). While Ukraine sought further alignment with the west, it still had to contend both with the major adversary on its border (Johansmeyer, Mott, & Nurse, 2025) and a western cohort viewing Ukraine through a narrow, regional lens influenced in large part by the Obama Doctrine, which gave some weight to Ukraine's historical role within Russia's sphere of influence (Pavlovych & Vasyolovych, 2019). This intensified a sense that Ukraine's interest in deeper integration with the West would struggle to be requited, not just because of the requirements associated with joining the likes of NATO and the EU. Rather, it seemed that Western powers perceived Ukraine as having a more complicated relationship with Russia than other states in the region (Pavlovych & Vasyolovych, 2019), a tendency that aligned with Russia's stated view regarding the historical interrelationship it has shared with Ukraine (Putin, 2021).

Of course, how the West responded to the 2021 essay by Russian President Vladimir Putin on that interrelationship heralded a change in potential support for Ukraine, and the invasion half a year later made the Russia/United States security balance that Ukraine had managed utterly unnecessary. The characterisation of Russia and Ukraine as "one people" (Wilson, 2021) clearly is intended to create a philosophical and historical underpinning for driving "what he [Putin] sees as the unity of the Russian and Ukrainian peoples" (Khvostunova, 2024), in a manner that costs Ukraine its sovereignty (Domańska, 2021). However, a post-war environment is likely to bring a return of the strategic balancing act in which Ukraine has had to engage. A tenuous peace (or at least non-war) would require Ukraine to avoid any perceived provocation that could result in another invasion, and the likelihood of partial Western support would require some amount of independence in that endeavour, essentially signalling a return to the status quo identified by Zahorulko (2020).

Future cyber security strategy is likely to focus on Ukraine's need for security partnerships and broader assistance. However, the limited effectiveness

of cyber war in general (Mueller et al., 2023: 16) and the empirical evidence of this arising from the aspects of the Russia-Ukraine war in the cyber domain (Beecroft, 2022) justify the reduced securitisation of cyber relative to the core threats involving an adversary on the border. Cyber security is important, as the need for the defence ultimately delivered by western states from late 2021 reveals (Austin & Khaniejo, 2023). On a standalone basis, though, it is not existential. The next NCSS will doubtless include heavy use of partnerships (and alliances where possible), but it should do so within a broader framework of managing smaller forms of cyber harassment and engagement within the context of the larger physical and military threat from next door.

RESEARCH METHODOLOGY

In order to evaluate the cyber war experiences of Ukraine since the 2022 Russian invasion – and to a lesser extent since the 2014 invasion – for the purposes of determining key considerations for Ukraine's next NCSS, this article uses publicly available expert analysis to understand how the cyber threats Ukraine contemplated from 2016-2021 materialized shortly before and during the war with Russia that began in 2022. The A wide range of sources is used – to include academic journal and think tank articles and commentary – to provide a foundation for an interpretive approach to security studies by identifying the relevant themes from prevailing expert commentary relevant to Ukraine's opportunities to mature and improve its approach to cyber security strategy. This article focuses on cyber operations excluding information warfare. Although Ukraine will need a strategy to contend with information warfare and foreign influence following a cessation of hostilities in the current war, those efforts fall outside the scope of this research, because the nature of the threat and remediation are fundamentally different from the core cyber security challenges that are the focus of this article.

ANALYSIS

There is no doubt that Ukraine has sustained frequent and significant cyber attacks since 2014 and even more so since the 2022 invasion (Council on Foreign Relations [CFR], 2024). The use of offensive cyber operations formed a clear element of Russia's combined arms effort, although the lack of meaningful impact from cyber activity is impossible to ignore (CFR, 2024). The result is that cyber operations represent a low-impact but ongoing security threat, which requires a specific approach to strategy that eschews the easy answers associated with deterrence and instead adopts the nuance necessary to allocate security resources effectively. Although the 2021 draft NCSS did emphasize the need for

foreign support in countering a Russian cyber campaign (Johansmeyer, Mott, & Nurse, 2024: 49), the lofty and existential characterisation of the cyber threat in both that strategy and the 2020 NSS (which emphasised the importance of deterrence) fundamentally misgauged what a cyber campaign would really look like, particularly when compared to kinetic warfare.

To see where cyber fits into broader security strategy, it is helpful to consider the attacks on Ukraine's power grid since 2015 – with the attack that year considered to be the most impactful via the cyber domain. It led to the loss of power by approximately 230,000 for up to six hours (Johansmeyer, 2024a: 7). A 2016 attempt was less impactful (CFR, 2024). Russia launched another credible attempt in 2022 (O'Neill, 2022), which has been characterised as a near miss. However, it should be considered as such relative to a 2015 success that was of limited impact. To illustrate the difference between cyber and kinetic warfare, the Ukrainian grid did sustain significant damage in 2022. When cyber attacks failed, Russia turned to the certainty of kinetic warfare, which ultimately cost Ukraine 40% of its grid (Schulze & Kerttunen, 2023: 6). While it may be true that Ukraine's defensive cyber capabilities made a difference (Wolff, 2022), the grid itself remained vulnerable to attack (and ultimately was impaired).

The cyber attacks Ukraine experienced from 2014 may have been frequent and unrelenting (Wilde, 2024: 3), but they were also small, manageable, and of limited impact when they did land successfully – which is why the Russian cyber attacks were largely seen as ineffective (Lewis, 2022: 8–9). Therefore, while the frequency speaks to the need for cyber security strategy, the lack of attendant impact demonstrates the need for balance within Ukraine's broader security strategy work and next NSS refresh. Many researchers mistake frequency for severity, considering an "onslaught" (Alazab, 2022) to have occurred even when the impact of the underlying attacks has not been meaningful (Mueller et al., 2023: 7–8). While frequency of attack does provide important input for strategic planning, a high rate of manageable attacks should not be confused with operations that have meaningful impact, of which there arguably have been none (certainly none since 2014) (Lewis, 2022; Johansmeyer, 2024b). The two most frequent cases noted from this period are clearly lacking in effect. The 2015 cyber-induced power outage was extremely limited in reach (approximately 230,000 people) and duration (one to six hours) (European Parliament, 2022: 3). The other, NotPetya in 2017, caused only US$10 billion in worldwide economic damage (very small relative to other forms of disaster) (Johansmeyer, 2024c), with only 5.6% of that impacting Ukraine (Johansmeyer, 2024d).

This may seem like an overtly contrarian statement, but it has foundation in ongoing research about the ineffectiveness of cyber war in general and is supported by empirical evidence dating back to the 2007 operations targeting Estonia (Johansmeyer, Mott, & Nurse, 2024: 42). According to Aaron Brantly and Nataliya Brantly

(2024), there are certainly subjective impacts related to cyber operations, but they are implicitly muted in comparison to the objective effects, as shown in their consideration of the objective and subjective effects of both Stuxnet and Operation Glowing Symphony (Brantly & Brantly, 2024: 476–477).

The nature of the conflict in the cyber domain between Russia and Ukraine, which is quite likely to persist in some form after the cessation of kinetic warfare, clearly speaks to low intensity and high frequency, with objectives leaning toward harassment rather than causing long-lasting and meaningful damage. Whether it is the loss of power for up to six hours in Ukraine (Johansmeyer, 2024a: 7) or a brief cessation of trading on the Moscow Stock Exchange (Carnegie Endowment for International Peace, 2022), cyber operations are limited in duration and impact, as previously determined by Smeets (2018: 12).

An analysis on objective impact alone would suggest the de-securitisation of cyber, but the frequency of attack and a holistic view of security correctly counter that the focus and investment should be proportional to a known threat. However, when factoring in the subjective impacts discussed by Brantly and Brantly (2024: 476), some amount of securitisation is necessary, if only to account for psychological and societal effects, not to mention future implications for strategy. Cyber security should not be ignored, but the strategy should be suited to the challenge. Rather than leaning on deterrence, which featured in the 2020 draft NSS (Johansmeyer, Mott, & Nurse, 2024: 48) and remains a favourite among cyber powers (Smeets & Soesanto, 2020), Ukraine's future NCSS should be ready to contend with cyber as an irregular warfare capability that can be disruptive but not existential.

This situation actually favours a return to the delicate strategic balance that Ukraine was forced to achieve prior to the full-scale war – and even prior to the 2014 invasion. Although it is imperfect to have to accept limited harassing cyber fires from a strategic adversary, striking a balance that does not leave them exposed to cyber threats but clearly accounts for the broader physical threat on the border is likely to represent the most achievable and useful cyber security strategy approach available to Ukraine following a cessation of kinetic war.

THREE PILLARS FOR STRATEGIC SUCCESS IN THE CYBER DOMAIN

Ukraine's next NCSS will have to once again thread a familiar needle. Although the cyber attacks experienced from 2014 through the present have not themselves been impactful – at least in comparison to the kinetic engagement of the period, even before 2022 – there remains the concern that ongoing disruption can have continual economic effects that not only impair the productivity of

Ukrainian companies and government entities but also could lead to instability and unrest in contested areas where Russian minority populations are quite large – similar to the effects of foreign influence in areas like Moldova (Deen & Zweers, 2022).

For Ukraine, the balancing act is to ensure its ability to protect itself from a high volume of harassing digital fires (Bateman, 2022) and to a limited extent assert itself in the cyber domain, while not provoking Russia into a return to the full-scale war that began in February 2022. Given that cyber operations can be de-escalatory (Lonergan & Lonergan, 2022: 36), Ukraine should be able to integrate offensive cyber operations into its strategy without the risk of provocation. For day-to-day cyber skirmishes (offensive and defensive), Ukraine will need to plan built upon relative independence, with Western support for security planning and hardening (U.S. Department of State, 2022) and deeper collaboration with regard to larger and more meaningful threats involving Ukraine's sovereignty.

While there is much for Ukraine to digest and implement from even the cyber elements of the war since 2022, there are three foundational elements that should be included in the country's next NCSS. First, it should lead with a view on the securitisation and prioritisation of the cyber domain relative to the rest of its security strategy. Second, the NCSS should strike the right tone with regard to foreign security partnerships, using the framing of cyber above to determine roles and capabilities that can be developed domestically versus those that require external support. Third, the next NCSS should include an appropriate role for offensive cyber operations.

Prioritisation and positioning

The lessons from the last three years in particular, let alone the past eleven years overall, suggest the need for an evolution in how cyber threats are understood, prioritised, and addressed. The debate over the supposed severity of cyber war appears to have been settled, based on empirical evidence from the cyber war in Ukraine, reinforcing the view that cyber war is not a significant threat (Rid, 2011), rather than a pervasive and existential problem (Arquilla & Ronfeldt, 1993). In fact, the experience since 2022 suggests that the cyber domain is one of limited impact and a narrow range of transitory potential outcomes, making it a poor fit for deterrence – a strategy used for the cyber domain by Ukraine (Johansmeyer, Mott, & Nurse, 2024: 48) and by western cyber strategy in general (Lewis, 2023). The relative de-securitisation of cyber represents an important strategic prioritisation exercise for Ukraine. While the fears of an invasion several years ago have come to pass, the digital counterpart has not. While

cyber security is indeed important and does require its own strategy, the nature of the threat must be formed by experience and then addressed appropriately.

Within Ukraine's broader security strategy architecture, cyber security certainly belongs in the NSS, although in that document, it should be balanced along with other priorities on a relative basis. The NCSS should then reiterate the cyber positioning in the NSS as a way to frame the cyber strategy itself. Linkages between the NCSS and territorial considerations would of course be highly relevant in linking cyber security to the broader strategy, particularly with regard to the interplay between cyber security and territorial integrity in the security philosophy of its neighbour and principal adversary (Johansmeyer, Mott, & Nurse, 2025: 25–26). Ultimately, how cyber security fits into Ukraine's broader NSS should then frame the cyber security strategy itself, with the NCSS defining the role of cyber security as part of the overall, integrated NSS.

Balancing self-reliance and foreign security support

With a view to the proper prioritization of cyber security within its NSS and the determination of how to develop an effective NCSS within that broader strategic framework, Ukraine's most important objective will be to strike the right balance between self-sufficiency and reliance on foreign partners. Western states demonstrated that they are prepared to support Ukraine in the cyber domain beginning in late 2021, with contributions that reportedly limited the effectiveness of Russian cyber attacks ahead of the early 2022 full-scale invasion. While Ukraine may expect a certain amount of proactive and preventive support from the west with regard to future cyber and kinetic conflicts, there will be day-to-day cyber security matters that it will have to handle on its own.

Some of where the line between self-sufficiency and foreign partnership lies will be dictated to Ukraine, at least implicitly, with the limits of western support forming a salient starting point for identifying the need for self-sufficiency. This should not be a blunt process, though. Rather than note the limits of western support as the start of its own efforts, Ukraine will continue to engage in the diplomacy that has surrounded its foreign cyber security partnerships since the 2021 pre-invasion cyber attacks, as delineated in the 2021 draft NCSS (Johansmeyer, Mott, & Nurse, 2024: 49). The negotiation of where western powers will partner with Ukraine for matters of cyber security should include consideration of what Ukraine can realistically accomplish on its own, as well as the determination of any potential gaps between Ukraine's self-perception on its capabilities and the limits of western partnership.

Interestingly, the 2022 war and cyber activity that preceded it suggest that the most effective role for foreign partners regards defence, which does not necessarily imply a defensive posture. In late 2021, the support provided by US and

other Western states contributed significantly to Ukraine's defensive posture and its ability to minimise the effects of the Russian 'onslaught' (Alazab, 2022). While the offensive capabilities of Western powers may seem like the intuitive choice with regard to foreign cyber aid, Ukraine can expect some amount of halo effect from the 'hunt forward' operations of the US and its allies (Temple-Raston & Powers, 2023). That said, it may not make sense any longer for Ukraine to leave offensive cyber operations to its foreign partners.

Offensive cyber operations

Perhaps counterintuitively, the limited effectiveness of cyber operations observed in the ongoing war in Ukraine supports their use on an offensive basis by Ukraine after the war has ceased (if not concluded). Further, at that stage, Ukraine will have the opportunity to codify the role of offensive cyber operations in its next NCSS. Russia's activity in Ukraine from 2014–2022 shows the cases and circumstances where cyber operations can be useful – i.e., below the threshold of war and as an alternative to more serious (and riskier) provocation. This thinking creates a space for Ukraine to integrate offensive cyber operations into its NCSS as a response mechanism to similar harassment while managing downward the risk of escalation. In fact, broadening its cyber security strategy to include the judicious use of offensive cyber operations could help minimise Ukraine's reliance on partner states.

Ukraine has been constrained by a self-imposed prohibition on offensive cyber operations (Kvartsiana, 2023: 20), which one can trace back to concerns over balancing the threat from the east and the expectation of limited support from the west dating back to the country's achievement of its post-Soviet independence. The permitted use of offensive cyber operations – even if those capabilities were never to be used – could still be seen by Russia as a provocation. For this reason, there is a certain sensibility in taking that strategic alternative off the table, especially given the concern that western will to support Ukraine may not be limitless.

Precedent for Ukraine's intentional self-deprivation of a strategic alternative does exist. The restriction on offensive cyber operations that Ukraine has imposed on itself can be seen as similar to its 1994 agreement to transfer its nuclear warheads to Russia for elimination in exchange for security assurances from Russia (and the US and UK), through the Budapest Memorandum (Pifer, 2011). The comparison is imperfect given the tendency of some to improperly class cyber and nuclear weapons as being of similar potential effect (Lewis, 2023), but both do involve voluntarily conceding a potential security lever. With regard to cyber weapons and offensive cyber operations, though, the decision

has cost them a strategic alternative they could use on a day-to-day de-escalatory basis, while nuclear capabilities are exactly the opposite.

Adopting offensive cyber capabilities would increase Ukraine's self-sufficiency and manage one more area of reliance on foreign partners, such as NATO. The inclusion of offensive cyber capabilities is not necessarily at odds with Ukraine's need to balance its ability to absorb harassing attacks from Russia with a somewhat limited reliance from western cyber powers. The constraints on offensive cyber activity in the 2021 draft NCSS should be lifted, with the recognition that there has been some state involvement in such operations since the 2022 invasion (Kvartsiana, 2023: 20).

The presentation of a new perspective on offensive cyber operations will be crucial to its positioning relative to Russian political and military readers of the next NCSS. Rather than simply increase the scope of its permitted activity in the cyber domain, Ukraine would be prudent to frame the expansion as quite limited in practice, with permitted operations specified rather than simply a focus on action (even if the former invariably brings the latter), recognition that cyber operations are of limited strategic military value and thus inherently less provocative than traditional deterrence measures, and finally that doing so may reduce its reliance on NATO and other, more powerful adversaries of Russia. Even with NATO reaffirming that Ukraine's future is in NATO and that they will continue to support it on its irreversible path to full Euro-Atlantic integration (NATO, 2024a), it is clear that eventual membership is far from guaranteed, as it will come only when "Allies agree and conditions are met" (NATO, 2024b). At a minimum, a seemingly reduced reliance on NATO may at least help Ukraine buy some time while working on longer-term and multi-national security solutions.

CONCLUSION

When the current conflict ceases – whether temporarily or permanently – Ukraine will need to revisit its entire NSS framework, both for a general refresh and to integrate the lessons from what will be at least three years of war with a larger and more powerful directly adjacent neighbour. Its previous strategy documents were developed during a period of conflict with Russia, but that conflict was limited and largely irregular. Since then, Ukraine has experienced an invasion and even invaded its adversary (i.e., Kursk; Evans, 2025). The kinetic war and attendant cyber engagements may call for a complete reimagining of Ukraine's approach to security strategy, but it also recalls a traditional challenge for the country, in which it must manage the risk of provoking its immediate adversary while trying to engage prospective western partners, an act itself that Russia could decide to be provocative.

With regard to its NCSS, Ukraine should first remember the general ineffectiveness of the cyber war since 2022, as well as the limited results such attacks gained for Russia from 2014 until the full-scale invasion. This is a lesson in threshold, and the fact that cyber attacks have been effective only below the threshold of war suggests an opportunity for Ukraine to evolve its thinking on offensive cyber operations. The war it has fought for more than three years (as of this writing) reveals that this dated perspective on offensive cyber operations is unwarranted. In fact, cyber operations are largely believed to have the potential to be de-escalatory. This, in conjunction with empirical evidence on the limited effectiveness of cyber warfare since late 2021 (and indeed since 2014), reveals the important role offensive cyber operations could play in the first post-conflict NCSS that Ukraine develops.

For this reason, Ukraine would be prudent to consider the three cyber security strategy pillars recommended in this article, based on the analysis of Ukraine's past NCSS and NSS, as well as the impact of the cyber engagements throughout the war. Foundational will be to prioritise and position cyber security appropriately overall within the country's NSS framework. Over-securitisation would ignore the salient lessons of the conflict, and over-prioritisation would fail to reflect the threats the country faces from its neighbouring adversary. Balancing foreign partnerships, especially with the US and NATO, is intended to ensure that Ukraine benefits from these relationships without turning those relationships into a reason for Russia to resume aggression. Finally, allowing itself the strategic alternative of offensive cyber operations, while seemingly inherently provocative, may create at least the appearance of a reduced reliance on foreign partners and provide other potentially de-escalatory benefits.

Of course, Ukraine will still need to proceed with foreign partnerships, to include alignment and cooperation with NATO, understanding that full membership may not come for several years (if at all). However, the judicious use of offensive operations in its NCSS, and perhaps in the wires, may help Ukraine control more of its fate, and in doing so reduce the risk of provocation associated with NATO collaboration. One should not expect this to be a complete solution to the issue of NATO and Russia, but it at least offers an opportunity, if documented in the NCSS, to offer a seeming concession, and in negotiations, perception matters.

REFERENCES

Alazab, M. (2022, February 24). *Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities*. The Conversation. https://theconversation.com/russia-is-using-an-onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165. https://doi.org/10.1080/01495939308402915

Beecroft, N. (2022, November 3). *Evaluating the international support to Ukrainian cyber defense*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en

Brantly, A., & Brantly, N. (2024). The bitskrieg that was and wasn't: The military and intelligence implications of cyber operations during Russia's war on Ukraine. *Intelligence and National Security, 39*(3), 473–482. https://doi.org/10.1080/02684527.2024.2321693

Council on Foreign Relations. (2024). *Cyber operations tracker*. https://www.cfr.org/cyber-operations/

Davydiuk, A., & Potii, O. (2024). *National cybersecurity governance: Ukraine*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf

Dickinson, P. (2021, July 15). *Putin's new Ukraine essay reveals imperial ambitions*. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/putins-new-ukraine-essay-reveals-imperial-ambitions/

Dickinson, P. (2024, November 26). *Putin's Ukraine obsession began 20 years ago with the Orange Revolution*. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/putins-ukraine-obsession-began-20-years-ago-with-the-orange-revolution/

Johansmeyer, T. (2024, April 5). *Why natural catastrophes will always be worse than cyber catastrophes*. War on the Rocks. https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/

Johansmeyer, T. (2024, April 10). *Debunking NotPetya's cyber catastrophe myth*. BindingHook. https://bindinghook.com/articles-binding-edge/debunking-notpetyas-cyber-catastrophe-myth/

Johansmeyer, T. (2024). If cyber is uninsurable, the United States has a major strategy problem. *Journal of Risk Management and Insurance, 28*(2), 7. https://jrmi.au.edu/index.php/jrmi/article/view/291/190

Johansmeyer, T., Mott, G., & Nurse, J. R. C. (2024). *Invisible lines, visible impact: How territorial security influences Russian cyber security strategy*. *RUSI Journal, 170*(1), 25–49. https://doi.org/10.1080/03071847.2025.2458143

Johansmeyer, T., Mott, G., & Nurse, J. R. C. (2024). Cyber Strategy in Practice: The evolution of US, Russian, and Ukrainian national cyber-security strategies through the experience of war. The RUSI Journal, 169(3), 40–51. https://doi.org/10.1080/03071847.2024.2377544

Kvartsiana, K. (2023, December). *Ukraine's cyber defense: Lessons in resilience*. German Marshall Fund of the United States. https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf

Lewis, J. A. (2022, June). *Cyber war and Ukraine*. Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine

Lewis, J. A. (2023, November 15). *Deterrence and cyber strategy*. Center for Strategic and International Studies. https://www.csis.org/analysis/deterrence-and-cyber-strategy

Lonergan, E. D., & Lonergan, S. W. (2022). Cyber operations, accommodative signaling, and the de-escalation of international crises. *Security Studies, 31*(1), 36–67. https://doi.org/10.1080/09636412.2022.2040584

Mitchell, C. (2008). The right moment: Notes on four models of "ripeness." *Paradigms, 9*(2), 38–52. https://doi.org/10.1080/13600829508443085

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, July). *Cyber operations during the Russo-Ukrainian war: From strange patterns to alternative futures*. Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

National Security and Defense Council of Ukraine. (2021, March 4). *The working group at the NCCC at the NSDC of Ukraine approved the draft Cybersecurity Strategy of Ukraine*. https://www.rnbo.gov.ua/en/Diialnist/4838.html

National Security Strategy of Ukraine. (2020). https://niss.gov.ua/sites/default/files/2015-01/Draft_strategy.pdf

Office of the Spokesperson. (2022, May 10). *U.S. support for connectivity and cybersecurity in Ukraine*. U.S. Department of State. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

Rid, T. (2011). Cyber war will not take place. *Journal of Strategic Studies, 35*(2), 5–32. https://doi.org/10.1080/01402390.2011.608939

Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies, 41*(1–2), 6–32. https://doi.org/10.1080/01402390.2017.1288107

Trenin, D. (2014, July 9). *The Ukraine crisis and the resumption of great-power rivalry*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2014/10/the-ukraine-crisis-and-the-resumption-of-great-power-rivalry?lang=en

Walker, N. (2023, August 22). *Conflict in Ukraine: A timeline (2014–eve of 2022 invasion)*. House of Commons Library. https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf

Zartman, I. W. (2001). The timing of peace initiatives: Mutually hurting stalemates and ripe moments. *The Global Review of Ethnopolitics, 1*(1), 8–18. https://doi.org/10.1080/14718800108405087

Zahorulko, A. (2020). National security strategy of Ukraine: Conceptual principles and efficiency. *Croatian and Comparative Public Administration, 20*(4), 679–699. https://doi.org/10.31297/hkju.20.4.4