International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)
Vol. 16, No.1/2 June 2025

SECURITY, DEFENCE AND CYBER SECURITY IN THE DIGITAL AGE

Zhiyuan Liu

School of computing and communications, Lancaster university, Lancaster, UK

ABSTRACT

This article, written in March 2023, examines the evolving relationship between society and technology—two forces that are deeply intertwined and continually influence each other, particularly in the digital age. The author begins with a quick review of globalization and the development of information technology and explain the definitions of key terms in this article. Using the ongoing war in Ukraine as a case study, the article explores hyperconnectivity as a future threat and reimagines cybersecurity within this evolving context, taking into account emerging technologies, societal attitudes, and the global geopolitical landscape. The role and impact of emerging technologies such as New Paradigm of cyberattacks, TikTok, UAVs, and star chains are discussed in detail. The article analyses grey areas in the digital age, the dynamics of real-time information and truth, organizational silos, infrastructure dependency, and worst-case scenarios through the lens of current events. In addition, this article provides suggestions on cybersecurity challenges in the current context from both technical and humanistic perspectives.

KEYWORDS

Cyber-attack, Fake News, Over-connectivity, Real Time, Soils, Starlink, TikTok War, UAV

1. INTRODUCTION

Over-dependence on digital connectivity Often referred to as Over-Connected or over-connectivity. In the past decade, new technologies in computing and communications such as distributed computing, Internet of Things technologies, virtual and augmented reality, and 5g technologies have evolved significantly. These technologies have redefined the paradigm and made human activity more dependent on digital connectivity. On the one hand, the digital revolution has enhanced the efficiency of human society and access to information. On the other hand, the threats posed by over-connectivity in the future are becoming clear. Bill Davidow, for example, claims that the Internet played a catalytic role in the global economic crisis due to the worldwide digitalization process, which allowed information to be disseminated quickly, cheaply, and reliably [1].

Three-time Pulitzer Prize winner Thomas Friedman claims in his book that the world entered “Globalization 3.0” in 2000—a phase of globalization driven by digital connectivity [2]. His book The World Is Flat was published in 2005, during the emergence of a new wave of global integration. However, in the following decade, the development of information technology such as artificial intelligence has enabled highly repetitive work to be further replaced by emerging productivity. This has led to a shift in many outsourcing industries from being labor-intensive to technology-intensive, significantly impacting large service-oriented countries like India. The globalization brought about by digital connectivity has also harmed industrial workers in developed countries, fueled populist movements and led to events such as the election of Trump, Brexit, and the US-China trade war. The ongoing war in Ukraine presents an even greater

DOI: 10.5121/ijmpict.2025.16201

challenge to globalization. Although globalization and its reversal driven by digital connectivity are not the main causes of the Russo-Ukrainian war, the tense international political and economic climate in recent years has clearly contributed to its outbreak. In addition, digital technology continues to play a pivotal role in this war.

1.1. Definition of Terms

The article defines overdependence on digital connectivity as the condition in which most people around the world are digitally connected and rely on this connectivity to live, work, and learn. This article acknowledges the contributions of digital connectivity but also critically examines the risks that overconnectivity may pose in the future.

The Oxford Dictionary defines “future” as a time after the present or as an event that is yet to occur [3].

The “cone of plausibility” was first publicly introduced by Charles Taylor [24] in 1988 to help researchers explore geopolitical scenarios. The concept visualizes the relationship between the present and the likelihood of future events. In this figure, the outermost category, “POSSIBLE,” represents the broadest range of scenarios, encompassing all conceivable outcomes. “Plausible” futures are more likely than those merely considered “possible,” but they require present-day changes and actions to materialize. “Probable” futures are those likely to occur based on current knowledge and observable trends, assuming no unforeseen disruptions. The "preferable" futures are the futures that researchers desire. Therefore, envisioning and planning for the future must be grounded in the present, as a researcher’s careful and honest examination of current conditions is essential to navigating potential futures.

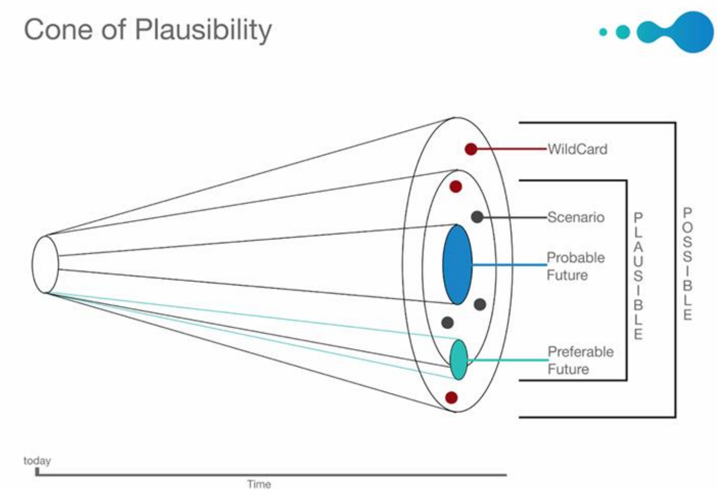

Figure 1. Cone of plausibility [24]

1.2. Research Background and Significance

Compared to the Iraq War, which is recognized as a prototype of digital warfare, the Russo-Ukrainian war delves deeper into the “grey zone”. Due to widespread digital connectivity, Ukraine has acquired front-line intelligence on Russian forces and increased international support by involving ordinary citizens in military activities. From another perspective, researchers should note that Russia is also deploying civilian cyber forces against Ukraine and the international community.

With Ukrainian and international volunteers participating in combat in unprecedented ways, the boundary between military and civilian actors has become increasingly blurred. Therefore, how the rules of warfare adapt to modern realities and how to protect human rights during conflict must be re-evaluated. In addition, the Russo-Ukrainian conflict has generated a wealth of data that can assist commanders in planning future deployments and documenting evidence to hold war criminals accountable. However, since the onset of the war, disinformation has flooded cyberspace, posing significant challenges to accurate data analysis and storage.

It is evident that current security and defense challenges are evolving alongside the continued informatization of society. At the same time, cybersecurity will be redefined within this emerging security landscape. According to Chandra Mukerji [4], humans must understand changes in social existence because the rapid pace of technological advancement has created new ways of being. By understanding the interplay between social and technological domains, researchers can more effectively analyze emerging threats. Therefore, this article will discuss the overreliance on digital connectivity and the possible future threats in the context of the current Russo-Ukraine war.

2. FROM TRADITIONAL CYBER ATTACKS TO THE "IT" ARMY

Prior to the invasion of Ukraine by Russian armed forces, various Ukrainian military and political institutions, key sectors such as energy and banking were attacked by DDoS and data-wiping malware originating from Russia. Global advanced persistent threat (APT) behavioral mapping data indicates that the Russian hacker group Gamaredon began conducting persistent, large-scale cyberattacks against Ukraine as early as December 2021, with activity peaking in February 2022 [5].

In 2022, Russian cyberattacks on Ukraine increased by 250% compared to 2020. During the same period, NATO countries experienced an increase of over 300% [6]. The Russians primarily targeted Ukrainian military and government sectors, as well as public utilities, infrastructure, and media.

Russia's massive cyber-attacks were quickly responded to. Shortly after the start of the war, Ukrainian Deputy Prime Minister Mykhailo Fedorov called on Twitter for talents in the digital field to join Ukraine's "IT army" and "fight" against Russia, and volunteers were organized via Telegram to complete tasks [7]. Volunteers simply needed to click “Join” on a specific Telegram channel to access their missions, which targets the websites of the Russian government, military agencies, banks, energy ministries, etc. Hacker groups, including Anonymous, have supported Ukraine independently, but the government-led IT volunteer army is unprecedented. More than 400,000 volunteers may have joined the effort, according to the Wall Street Journal [8].

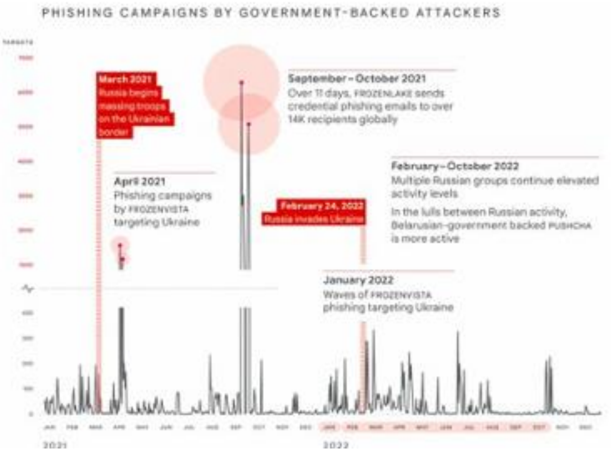

Figure 2. Polishing Campaigns by Government-Backed Attackers[25]

Interestingly, in addition to traditional cyber operations, Ukrainian missions also involve reporting YouTube channels spreading war-related misinformation, making it possible for volunteers with limited Internet skills to complete the corresponding work.

However, Tim Stevens of King’s College London [9] stated that the potential for escalation in cyber conflicts is concerning. The involvement of non-Ukrainians and non-Russians in cyberattacks could internationalize and escalate the conflict beyond Ukraine’s borders. At the same time, the effectiveness of the IT army is difficult to quantify due to the anonymity of the volunteers involved. Ukraine’s IT army has broken the silo mentality; however, constructing a coordinated organizational network remains a major challenge.

Although Russia has conducted high-intensity cyberattacks, these contributed little to its military operations during the stalemate phase of the war. Before the war, Russia disrupted the Viasat satellite communication network. However, subsequent cyberattacks had limited destructive impact, and their frequency declined sharply in March 2022. According to experts at the Carnegie Foundation, Russia’s limited cyber capabilities, institutional weaknesses, and the resilience of Ukraine and its allies have contributed to its underwhelming cyber performance [10]. Technical and political constraints have prevented Russia from executing cyber operations in a precision- and intelligence-driven manner.

3. REAL-TIME WAR AND RUMORS

3.1. Tiktok War

The physical war remains unresolved, yet Ukraine has achieved a landslide victory on social media. Live broadcasts, memes, and video clips captured the attention of netizens around the world. The Russo-Ukrainian war is also considered the first “TikTok war”, as the social media platform played a role in the early stages of the war. At the same time the Russian army began its attack, a large volume of psychological warfare videos appeared on TikTok for a short time. For example, planes and tanks in combat are shown. The text in these videos shows that Kyiv had been captured, among other claims. A mobilization video from Chechnya, Russia, also spread rapidly on the internet. Due to historical events and cultural backgrounds, Chechen soldiers are considered by many to be fearsome soldiers. There is no doubt that the main purpose of producing this content is to undermine the confidence of the Ukrainian resistance. Jon

Roozenbeek, a postdoctoral fellow in psychology at the University of Cambridge, has found that the Kremlin is adept at deploying effective psychological manipulation tactics through social and online media, including belittling hostile groups and rapidly spreading falsehoods [11]. However, Moscow's tactics quickly failed as Ukraine's leadership and citizens emerged on social media.

President Zelensky is arguably the most iconic Ukrainian online figure, with dramatic daily updates via Twitter. The president, with a background in acting, has shown a deep understanding of the impact of new media and social networks, and has quickly assumed superhero roles and global stardom, much of it just through his phone. His work helped resist Moscow’s disinformation, such as the flight of senior Ukrainian officials abroad, stabilize the resolve of the Ukrainian people and garner international sympathy and support, making Ukraine a David against Goliath. Audio of a Ukrainian soldier remaining on Snake Island in the Black Sea refusing to evacuate and shouting 'Russian warship, go f** yourself' went viral online, to the extent that it became a global meme and symbol of resistance in Ukraine [12].

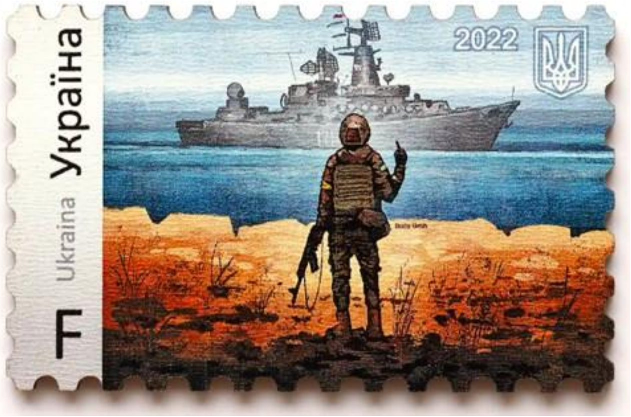

Figure 3 The Meme and stamp[26]

The Arab Spring of 2011 is widely seen as the first revolutionary movement based on social media, but smartphones were far less ubiquitous than they are today. In recent years, smartphones have been widely used, and 4G and 5G technologies have provided the infrastructure for real-time capture and live broadcast. In the days leading up to the official Russian military offensive, TikTok users posted videos showing Russian troops massing on the border, though Russia initially denied launching an attack on Ukraine. As the war progressed, social media platforms began to become tools for collecting evidence of the war and helping to hold it accountable. According to NBC NEWS[13], U.S. politicians sent letters to Meta, TikTok, Twitter, and YouTube in May 2022, asking these companies to archive potential evidence of Russia’s war crimes in Ukraine. The letters are not legally binding, but the authors were senior Democrats and thus enjoy considerable political support. Ukraine has also rolled out a special chatbot that allows the public to report movements of enemy troops and military equipment. The tool is integrated into the widely used Diia application, which has attracted more than 460,000 Ukrainian users. The reports they provided helped destroy dozens of Russian military positions as well as tanks and artillery [14]. The Diia app was released by the Ukrainian government in February 2020 to eliminate bureaucracy and digitize key government departments.

3.2. The True and the False of Social Media

However, the authenticity of real-time war information disseminated via digital media warrants critical attention. In the early days of the war, fake live broadcasts, game clips, military exercises, and old videos tagged with real-time information from the battlefield were widely circulated. For example, the video of the Ukrainian combat pilot "Ghost of Kyiv" was widely circulated on TikTok and Twitter. The video actually originated from footage of the video game Digital Combat Simulator. The New York Times [15] reported that the 'Ghost of Kyiv' was likely a product of mythmaking and propaganda, endorsed by, and sometimes derived from, Ukraine's official social media channels. Given that teens make up a large percentage of TikTok's users and rely on the app. The spread of misinformation is deeply troubling. Emotional content and a dopamine rush make viewers lose sight of whether the video content is authentic and legitimate. The real purpose of fake content is to try to elicit an emotional response and go viral. Some counterfeiters even exploited public sympathy for Ukraine to solicit donations for personal gain.

TikTok's powerful recommendation algorithm provides viewers with content aligned to their preferences, and the war hashtag in Ukraine is particularly eye-catching. A study by the fact-checking group NewsGuard [16] showed that fake news stories about the war in Ukraine were recommended to new TikTok users within 40 minutes of signing up, and by the end of the 45-minute experiment, the recommendations were almost exclusively about the war in Ukraine. The content of these news stories is a mix of true and false information, so it was difficult at that time to distinguish between true and false content or identify reliable sources on TikTok. TikTok subsequently stated that they would eliminate harmful false information and cooperate with independent fact-checking organizations to ensure TikTok's safety and authenticity. However, numerous fake videos have previously damaged TikTok’s reputation, and except in cases where profiting from fake news constitutes a clear crime, the primary consequence for others is often limited to account suspension or deletion. Therefore, the international community still faces significant challenges in reducing the influence of fake news on social media and holding offenders accountable.

4. UAV AND STARLINK IN THE WAR

IoT devices, particularly UAVs, played a prominent role in the war in Ukraine. According to Defence News, the traditional U.S. military perspective holds that conventional UAVs are ill-suited for future warfare. Therefore, the U.S. military has emphasized advanced performance such as stealth and high speed for the next generation of UAVs, which has caused a substantial increase in the cost of UAVs [17].

In the war, this view was fundamentally challenged. In the early days of the war, facing the full range of Russian air defence systems, Ukrainian force use the Turkish-made TB-2 UAVs to launch frequent attacks on the Russian army stationed on Snake Island, which forced the Russian army command to consider the combat cost and ultimately abandoned the island. In addition, the TB- 2 UAVs also played an important role in the sinking of the cruiser "Moscow", the flagship of the Black Sea Fleet. However, by the end of May 2022, at least 90 TB2 UAVs were destroyed by air defence forces. This conventional military drone has several weaknesses, including large size, slow speed, and low altitude flight, and its replacement cost is approximately 2 million USD. As a result, warring parties have turned to unconventional drones for combat. These small UAVs are well-suited for individual reconnaissance missions. While the Russian army waited for the order to fire, the Ukrainian army had already made a quick decision through an application downloaded to the smartphone. This operational model enables real-time data transmission to long-range systems such as artillery that is closest to the drone. In addition, commercial drones can be easily modified to perform combat missions. On the front line of the Russia-Ukraine conflict, both sides frequently deploy tactical-level squads for offensive and defensive operations along the contact line. For such small targets, individual drones can achieve better strike effects. Even with limited precision, they can instil fear in ground troops. However, commercial drones are far less capable than military drones. For instance, the DJI Mavic has a maximum flight range of only 30 kilometres, and it can only fly for 46 minutes at most. In addition, commercial drones are easily jammed by electronic devices. Russia uses weapons capable of emitting electromagnetic pulses that could prevent commercial drones from using GPS for navigation.

Ukrainian UAVs have benefited from technical and geolocation support provided by Starlink. Musk's Starlink system began taking over communications in Ukraine shortly after Russian forces disrupted Ukraine’s terrestrial internet infrastructure and mobile phone network. This became the first use of Starlink in warfare. The Ukrainian government has distributed Starlink terminals to government departments, Ukrainian military command structures, Ukrainian frontline units, critical infrastructure, etc., making Starlink an important communication channel for Ukraine.

Starlink's signal is stronger, more resistant to interference, offers higher transmission speeds and requires less power to operate than other satellite communications networks. On the civilian side, Starlink restored the mobile phone communication network, which made it possible for the public to transmit information about Russian military activities through mobile phones, enabling a communication chain from mobile device → Starlink network → Ukrainian government chatbot → military intelligence → combat troops. Although Starlink is a civilian system, it possesses capabilities applicable to the military domain. Starlink can provide military communication services covering the world, and as a data exchange platform and communication relay node for unmanned systems. In addition, Starlink has all-weather, all-day space-based reconnaissance and surveillance capabilities, and its satellites can also emit omnidirectional beams to perform telemetry, tracking, and control of spacecraft. Therefore, researchers need to pay attention to its potential capabilities in battlefield reconnaissance, electronic countermeasures, anti-missile interception, and communication support.

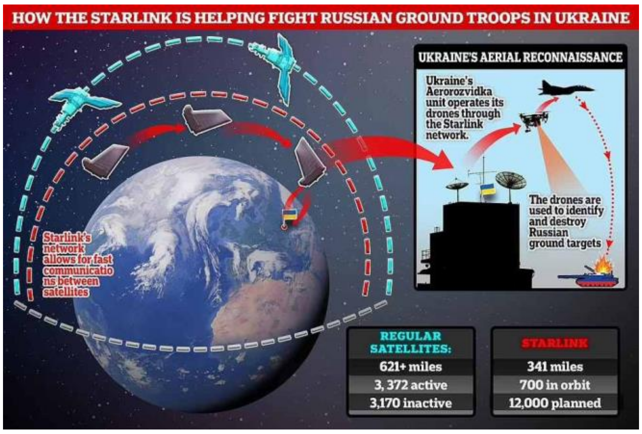
HOW THE STARLINK IS HELPING FIGHT RUSSIAN GROUND TROOPS IN UKRAINE
UKRAINE'S AERIAL RECONNAISSANCE
Ukraine's Aerorozvidka unit operates its drones through the Starlink network.
The drones are used to identify and destroy Russian ground targets
Starlink's network allows for fast communicatio ns between satellites
REGULAR SATELLITES:
621+ miles
3, 372 active
3,170 inactive
STARLINK
341 miles
700 in orbit
12,000 planned

Figure 4. Military uses of Starlink[27]

4.1. The Epoch-Making Significance of Starlink

The most important contribution of Starlink is its ability to break down the silos of the old system. The term silo mentality is often used to describe different departments within the same enterprise operating independently and avoiding sharing information, as well as in business units constrained by system limitations. This mindset is believed to hinder organizational effectiveness. In a siloed culture, it is difficult for individuals to collaborate with others and implement significant change. Individuals make decisions on their own terms without seeing the motivation to make changes of their own to help solve others' problems [18].

Starlink technology has transformed the legacy system into an integrated network. For example, the Ukrainian army has realized instant communication on the battlefield and can disseminate real-time information. The Ukrainian army's command system can access precise coordinates, ammunition status and firing direction of Ukrainian heavy firepower units.

As a result, the Ukrainian army can deploy single artillery units across the battlefield, achieving decentralization and avoiding Russian attacks. At the same time, the scattered Ukrainian single-door artillery can fire at the target at a different time according to the distance, bullet speed, and trajectory, in order to synchronize impact timing on the target, under the real-time coordination of the Ukrainian army command system. This has increased the cost of Russian force deployments and complicated the execution of large-scale offensives. Ukrainian military has established an operational chain of reconnaissance platforms → command and control systems → Starlink network → strike forces. It can be seen that the Starlink satellites have played a link role in realizing the OODA loop (Observe, Orient, Decide, Act) in executing precision strikes and targeted decapitation operations.

4.2. Hidden Dangers of Starlink

However, the widespread use of the Starlink system has also revealed hidden dangers during the war. From a political perspective, Starlink remains a civilian system, but Ukraine has been using Starlink for military operations on a large scale. According to Reuters [19], on February 8, 2023, SpaceX President Gwynne Shotwell stated that SpaceX had taken measures to prevent the Ukrainian military from using its Starlink satellite internet service to control drones during the war with Russia. Since SpaceX's original intention was to provide broadband communications to assist Ukraine's defense against Russian forces, it was never meant to be weaponized. The agreement between SpaceX and the Ukrainian government was originally intended for humanitarian purposes. SpaceX did not explain why Starlink suffered a service outage in Ukraine late last year. Musk later stated that Starlink remains Ukraine's communications backbone, but SpaceX would not allow its involvement to escalate the conflict into World War III [20]. As early as September 2022, Musk tweeted that Starlink's terms of use clearly stipulated that it should not be used for military activities. At present, the use of commercial satellites for military activities is a grey area of international law. While Starlink has supported Ukraine's resistance, determining its appropriate use still requires negotiations between the Ukrainian government, SpaceX, and the U.S. government.

From an economic perspective, SpaceX is a modern for-profit enterprise, and funding Ukraine represents a significant financial burden. CNN reported exclusively that, on October 14, 2022, Musk stated he would no longer fund for the Starlink service provided to Ukraine and requested that the U.S. Department of Defense cover the related costs [21]. SpaceX has spent about $80 million supporting Ukraine, he added. SpaceX sent a letter to the U.S. Department of Defense last month, emphasizing its inability to continue funding Ukraine's Starlink network and exploring the possibility of receiving U.S. Department of Defense support. The White House has provided Ukraine with tens of billions in various aids and arms manufacturers have received Pentagon fees. However, SpaceX, which facilitates communications between these systems, has not received direct financial compensation.

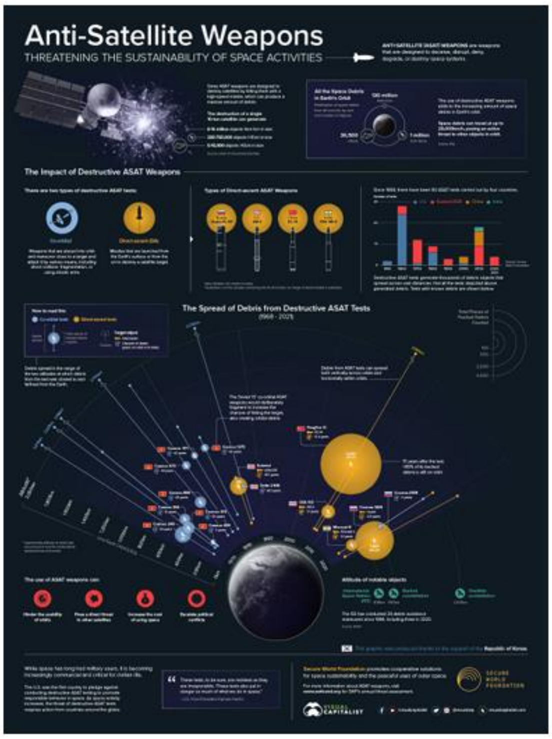
Anti-Satellite Weapons
THREATENING THE SUSTAINABILITY OF SPACE ACTIVITIES
The Impact of Destructive ASAT Weapons
The Spread of Debris from Destructive ASAT Tests
(1968 - 2021)

Figure 5. Anti-Satellite Weapons[28]

From a technical perspective, most satellite constellations operate in low Earth orbit, so Russia has the ability to destroy them. While a direct Russian attack on U.S. satellites is unlikely, it is highly probable that Russia will retaliate in other ways. Konstantin Vorontsov [22], deputy director of the Department of Non-proliferation and Arms of the Russian Ministry of Foreign Affairs, once said that the space arms race is heating up and quasi-civilian infrastructure may become a legitimate target of retaliation. While he didn't explicitly name a specific target, there was no doubt that he was referring to Starlink. In November 2021, Russia destroyed one of its old satellites to demonstrate its space combat capabilities.[23] In addition, according to CNN [21], the Ukrainian commander-in-chief Zaluzhniy said in July 2022 that about 500 Starlink terminals were destroyed in battles every month and requested nearly 8,000 more "Starlink" terminals. This indirectly suggests that Starlink terminals are vulnerable to battlefield losses. In January 2023, the Russian army's attack on Bakhmut suddenly accelerated, and its coordination ability was greatly improved, which also shows that the Russian army has gained a certain advantage in electronic warfare.

5. Reimagining Cyber Security in the New Security and Defense Context

Considering the current degree of digitalization and the real performance on the Ukrainian battlefield, it is necessary to conceive and redefine cyber security. First, the fact that Russian cyberattacks often precede and accompany conventional military offensives suggests that cyberattacks will play an increasingly important role in future warfare. Therefore, at the national level, it is necessary to develop a robust national cyber defence system and cultivate sufficient cybersecurity professionals.

Second, the legal and ethical grey areas surrounding cyberattacks are becoming increasingly blurred. In the future, serious cyber attacks will be generally regarded as a method of warfare. The borderless nature of the digital environment extends the scope of the cyber battlefield beyond that of the physical battlefield. The proliferation of digital connectivity is also making the lines between civilians and soldiers less and less clear. Therefore, it is urgent for the international community to establish international laws governing warfare in the digital age, so as to avoid the expansion of wars and conflicts.

Then, social media has made warfare more immediate and transparent. How to utilize social media to combat disinformation and promote truth is a critical issue for politicians and scholars alike.

Next, Ukraine assembled a virtual command and control system that enabled the breakdown of organizational silos and the creation of a networked command structure. The U.S. military's ambitious digital infrastructure appears overly bureaucratic. The work in Ukraine provides lessons for future structural reforms of national militaries.

Finally, Starlink, originally intended for commercial use, played a critical role in the war. However, the system has been used multiple times in the military, and SpaceX, the Ukrainian military, and the U.S. military have engaged in several disputes regarding its use. Therefore, in the future, efforts should be made to limit the use of civilian and commercial systems in military operations whenever possible, and nations must ensure that the infrastructure they rely on remains stable and consistently available.

6. CONCLUSIONS

Digital technology has enabled widespread participation in shaping contemporary society, while also transforming the security and defence landscape. At the same time, the evolving security environment is redefining cybersecurity. Previously ambiguous grey areas are gradually becoming clearer, highlighting the need for laws and international consensus to evolve in step with technological change. Society and technology evolve together, each shaping and accelerating the progress of the other.

ACKNOWLEDGEMENTS

Zhiyuan Liu thanks School of computing and communications, Lancaster university.

REFERENCES

[1] Overconnected: The promise and threat of the internet: Leading blog: A leadership blog (no date)Overconnected: The Promise and Threat of the Internet | Leading blog: A Leadership Blog.

[2] Friedman, T.L. (2007) The World Is Flat: A Brief History of the twenty-First Century.Vancouver: Douglas & McIntyre.

[3] Future (no date) future_1 noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com.

[4] Mukerji, C. (2017) Modernity reimagined: An analytic guide. New York: Routlege.

[5] Huntley, S. (2023) Fog of war: How the Ukraine conflict transformed the cyber threat landscape, Google. Google. Available at: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine- conflict-transformed-the-cyber-threat-landscape/.

[6] Services.google.com (no date). Available at: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

[7] Serrano, J. (2022) Ukraine creates it army of volunteer hackers to fight Russia, Gizmodo. Gizmodo. Available at: https://gizmodo.com/ukraine-it-volunteer-hacker-army-response-to-russian-in 1848600395.

[8] Ukraine's 'it Army' has hundreds of thousands of hackers, Kyiv says (2022) The Wall Street Journal. Dow Jones & Company. Available at: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says RfpGa5zmLtavrot27OWX .

[9] Burgess, M. (2022) Ukraine's volunteer 'it Army' is hacking in uncharted territory, WIRED UK. Available at: https://www.wired.co.uk/article/ukraine-it-army-russia-war-cyberattacks-ddos.

[10] What the Russian invasion reveals about the future of cyber warfare ... (no date). Available at: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of- cyber warfare-pub-88667.

[11] Roozenbeek, J. (2019) Media and identity in wartime Donbas, 2014-2017, Apollo Home. University of Cambridge. Available at: https://www.repository.cam.ac.uk/handle/1810/305148.

[12] Russian warship, go fuck yourself': What happened next to the Ukrainians defending Snake Island? (2022) The Guardian. Guardian News and Media. Available at: https://www.theguardian.com/world/2022/nov/19/russian-warship-go-fuck-yourself-ukraine- snake island .

[13] Facebook, YouTube and TikTok asked by four House Committee Chairs to Archive War Crime Evidence (2022) NBCNews.com. NBCUniversal News Group. Available at: https://www.nbcnews.com/tech/internet/democrats-ask-facebook-youtube-archive- evidence-war crimes-rcna28563.

[14] Dickinson, P. (2023) Tech innovation helps Ukraine even the odds against Russia's military might, Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/tech-innovation helps-ukraine-even-the-odds-against-russias-military-might/.

[15] Thompson, S.A. and Alba, D. (2022) Fact and mythmaking blend in Ukraine's Information War, The New York Times. The New York Times. Available at:https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html.

[16] TikTok algorithm directs users to fake news about Ukraine War, study says (2022) The Guardian. Guardian News and Media. Available at: https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to- fake-news about-ukraine-war-study-says.

[17] Calcara, A. et al. (2022) Why drones have not revolutionized war: The enduring hider-finder competition in Air Warfare, MIT Press. MIT Press. Available at:https://direct.mit.edu/isec/article/46/4/130/111172/Why-Drones-Have-Not-Revolutionized- War

[18] What is the definition of silo mentality? (2019) Perception Dynamics. Available at: https://www.perceptiondynamics.info/silo-mentality/how-to-remove-silo-mentality/.

[19] Person and Roulette, J. (2023) SpaceX curbed Ukraine's use of Starlink Internet for Drones company president, Reuters. Thomson Reuters. Available at: https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet drones-company-president-2023-02-09/.

[20] Satariano, A. (2023) Elon Musk doesn't want his satellites to run Ukraine's drones., The New York Times. New York https://www.nytimes.com/2023/02/09/world/europe/elon- Times. Available at: musk-spacex-starlink-satellite ukraine.html.

[21] Marquardt, A. (2022) Exclusive: Musk's spacex says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab | CNN politics, CNN. Cable News Network. Available at: https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink ukraine/index.html .

[22] The hack that should have been impossible (no date) Bloomberg.com. Bloomberg. Available at: https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/.

[23] Quach, K. (2021) ISS crew shelters from debris after Russia blows up Old Sat, The Register® Biting hand that feeds IT. The Register. Available at: https://www.theregister.com/2021/11/16/russia_satellite_iss/.

[24] The cone of plausibility can assist your strategic planning process (no date) Prescient. Available at: https://prescient2050.com/the-cone-of-plausibility-can-assist-your-strategic-planning-process/

[25] Huntley, S. (2023) Fog of war: How the Ukraine conflict transformed the cyber threat landscape, Google. Google. Available at: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine- conflict-transformed-the-cyber-threat-landscape/

[26] 107 snake Island Ukraine stock photos, Images & Pictures (no date) 107 Snake Island Ukraine Stock Photos - Free & Royalty-Free Stock Photos from Dreamstime. Available at: https://www.dreamstime.com/photos-images/snake-island-ukraine.html

[27] Elon Musk's Starlink satellites helping Ukraine drones destroy Russian tanks (no date) Tech Startups Tech Companies Startups News. Available at: https://techstartups.com/2022/03/19/elon-musks-starlink-satellites-helping-ukrainian-aerorozvidka-drones-destroy-russian-tanks/

[28] Article & Editing and Graphics & Design (2022) Anti-satellite weapons: Threatening the future of Space Activities, Visual Capitalist. Available at: https://www.visualcapitalist.com/sp/anti-satellite-weapons/

AUTHORS

Zhiyuan Liu received the BSc degree in AI and Robotics from Aberystwyth University, UK, in 2022 and the MSc degree in Cyber Security from Lancaster University, UK, in 2023.