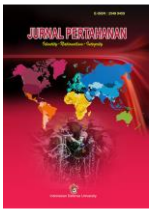
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



DB1000N SOFTWARE AS UKRAINE'S MILITARY UTILITY TO COUNTER RUSSIAN INVASION IN 2022

Muhammad Fikry Anshori
Japanese Area Studies, School of Strategic and Global Studies, University of Indonesia
Center for Japanese Studies, Prof. Dr. Selo Soemardjan Street, Depok, West Java, Indonesia 16424
muhammad.fikry01@alumni.ui.ac.id

Article Info

Article history:
Received : April 26, 2022
Revised : August 18, 2022
Accepted : August 19, 2022

Keywords:
Cyber Warfare,
Db1000n,
DDoS attack,
Military Utility,
2022 Russian Invasion of Ukraine

DOI:
http://dx.doi.org/10.33172/jp.v8i2.1683

Abstract

As Russia launched an invasion in every domain of warfare, including cyberspace, Ukraine employed an Information Technology (IT) army equipped with software called db1000n on March 2022. This article seeks to explain how the use of db1000n helps Ukraine against the 2022 Russian invasion. Using a case study as the research method and Susan Martin's military utility concept as the analytical framework, this article found that db1000n helps to support Ukraine's cyber warfare effort by being Distributed Denial of Service (DDoS) attack software that possesses three types of military utility, namely technical utility, tactical utility, and strategic utility. Nevertheless, db1000n still has some limitations that cannot secure an easy victory in cyber warfare.

INTRODUCTION

On February 24, 2022, Russia launched an invasion of Ukraine in every domain of warfare including cyberspace. Russian hackers had initiated attacks on many Ukrainian websites since the start of the invasion, making governments' web pages and online banking services could not be accessed by the public (Tidy, 2022). Ukraine's vice prime minister and minister for digital transformation responded to Russian attacks by creating an information technology (IT) army that comprised cyber security specialists on February 22, 2022 (Fedorov, 2022). This army's main task is to conduct cyberspace military operations against Russia's information infrastructure. On March 19, 2022, the Ukrainian IT army adopted a software named "death by 1000 needles" (db1000n) as a tool to support Ukraine's cyber warfare effort (IT Army of Ukraine, 2022c).

Db1000n is a recent case on military technology. Military technology has been an important part of warfare and winning it. Although there were scholars who argue that the morale of the troops is more important, the contribution of military technology to achieving victory in the battle cannot be simply dismissed (Cohen, 2018).

Many military technologies have transformed the domain of warfare as well, for instance the invention of tanks for land warfare, the development of submarines for naval warfare, and the innovation of planes for air warfare (Roland, 2016). Recent development in the information and communication sector opens up the possibility to conduct cyber warfare.

Db1000n is also a recent case of cyber warfare. There is no single definition to describe cyber warfare. Choucri (2012) defined cyber warfare as a range of offensive and defensive military activities in cyberspace to protect the states and its interest. On the other hand, Green (2015) stated that cyber warfare is an extension of policy taken by state or state-sponsored actors' in cyberspace as a response to foreign threats or to pose threats to another state. This article will refer to the cyber warfare definition by Lucas (2016) which states that cyber warfare is an attack carried out by state or non-state actors in cyberspace that causes substantial devastation to people and objects in the physical domain. Because db1000n software is a recent case on military technology and cyber warfare, this article proposes one research question, how does the use of db1000n help Ukraine against the Russian invasion? With this question, this article seeks to explain the use of db1000n by Ukraine in terms of military utility.

Several studies have been conducted on military technology, cyber warfare, and military utility in the last five years. Siroli (2018) discussed the dual use of hardware and software in the market for cyber warfare at the tactical, operational, and strategic levels. Meanwhile, Mori (2018) explored the Obama and Trump administration's efforts to develop artificial intelligence for defense and its implications for United States allies. Next, Schneider (2019) investigated the military revolution's dependency on computational technology which resulted in a vital vulnerability for states to engage in cyber warfare. In contrast, Mori (2019) compared China's military technologies innovation for cyber warfare and the United States military and industry countermeasures to deal with it. Later, Thornton & Miron (2020) examined the Russian military's use of artificial intelligence for autonomous propaganda, espionage, and destruction during cyber warfare. Last, Shandler, Gross, & Canetti (2021) surveyed the public perceptions in the United States, United Kingdom, and Israel towards the use of digital technology in cyber warfare.

This article will proceed as follows to answer the research question. First, this article presents the case study method and military utility concept used to examine db1000n in the 2022 Russian invasion. Then, this article analyzes data about the use of Ukraine's db1000n by operationalizing the military utility concept from Susan (Martin, 2016). Finally, this article concludes the findings and discussions on db1000n's military utility.

METHODS

The methods used in this article are qualitative in the form of a case study. This article fulfills three requirements to use a case study by Robert, namely research question in form of "how" or "why", the research does not require control over behavioral events, and the research focuses on contemporary events (Yin, 2017). The data collection techniques used in this article are internet-based studies and literature-based studies. With that data collection techniques, this study used the following data sources:

1. IT Army of Ukraine's Telegram channel
2. Db1000n GitHub repository
3. Office of the President of Ukraine website
4. Books or book chapters
5. Journal articles

This article operationalizes the following steps to analyze the collected data:

1. Setting an analytical framework from the concept
2. Categorizing the collected data based on the analytical framework

3. Creating a description or visualization of the collected data
4. Reflecting the coherency of the description or visualization with the analytical framework
5. Repeating step two, three, and four until getting the answer for the research question. Those five steps were adapted from the data analysis technique for the case study suggested by (Yin, 2017).

RESULT AND DISCUSSION

Military Utility

According to Chapman, Elbahtimy, & Martin (2018), military utility is an important concept in the study of international relations but is still rarely discussed. One of the scholars who keenly discusses the military utility concept is Susan Martin. Martin has been examining the military utility in various publications, namely the utility of biological weapons for deterrence (Martin, 2002); the utility of chemical, biological, and nuclear weapons in war (Martin, 2004); the constraint on the utility of nuclear weapons in international politics (Martin, 2013); and the military utility of chemical agents in Vietnam War (Martin, 2016).

Martin (2013) drew upon the structural realism approach to conceptualize military utility. Structural realism has three main ideas as follows (1) the structure of the international system is anarchy; (2) anarchy leads states to the self-help logic; and (3) self-help logic compels states to maximize their security or power (Dunne & Schmidt, 2019). Those three main ideas differentiate structural realism from the main ideas of classical realism which are the egoistic nature of humans determining international politics and national interest defined in terms of power (Dunne & Schmidt, 2019). According to Dunne & Schmidt (2019), both structural and classical realism still shared the same assumptions regarding statism, self-help, and survival

Martin (2016) argued that an anarchical understanding of the international system makes structural realism expect the military utility to become an essential factor in the state's decision in times of war. This is because the military utility has material characteristics (e.g. immense destructive power, ability to overcome defenses, and invulnerability to pre-emption) which cannot be taken away from how states will act in the international system (Martin, 2013). In addition, material consequences of a state's actions in international affairs have always become a structural realism priority (Brilmayer, 1999; Martin, 2004). Those logics serve as a foundation for Martin (2016) to conceptualize three types of military utility, which are technical utility, tactical utility, and strategic utility.

The technical utility is defined by Martin (2016) as to whether it works to have the desired result on thse target. The term ‘works’ in the definition is in a narrow sense, meaning the function or operation certainty. Martin (2016) gave three examples to illustrate the technical utility, such as a soldier's rifle may fail to discharge bullets, chemical agent spray may fail to have an effect, or aerial bombs may fail to detonate. It is relatively clear to asses technical utility compared with tactical utility and strategic utility for the reason that only focuses on mechanical aspects (Martin, 2016). Chapman et al. (2018) argued technical utility concerns about the general use of weapons. It is all about whether weapons can kill, injure, or destroy large numbers of troops or affect large areas assuming there is no influence from the target and environmental factors. The technical utility can also be understood as basic use, meaning ignoring the battlefield condition in the use of the weapon calculation (Chapman et al., 2018).

Moving forward to the second military utility, the tactical utility has relation to the context on the battlefield. Martin (2016) stated that something has tactical utility when it helps to achieve the user’s aims within the theatre of wars. Tactical utility concern whether it supports or not accomplishes objectives in the campaign (Martin, 2016). Hughes (1994) and Martin

(2016) also argued that tactical utility can become more difficult to exert because it is time-dependent. In that case, the tactical utility can be said to rest upon the actor's interest in the operation and the phase of the operation. Further elaboration on tactical utility has been done by Chapman et al. (2018). They defined tactical utility as the performance of the weapon on the battlefield. Chapman et al. (2018) gave five examples to illustrate the tactical utility, namely preventing the opponent to capture land, reaching an invulnerable target, undermining the morale of opponent troops, imposing logistical challenges for enemy in the battlefield, and maintaining battle objective in the course of operation.

The strategic utility is the last military utility identified by Martin (2016) which refers to whether it maintains the actor's broader goals. While tactical utility concentrates on the scope of the battlefield, the scope of strategic utility comprises political goals in international affairs (Martin, 2016), for instance:

1. sovereignty preservation of a nation;
2. military threats containment; and
3. prevention of further escalation against others.

In practice, decision-makers also take into consideration certain strategic utilities that will help further foreign policy in the long term. It is because the discussion of strategic utility has an association with the potential undesired costs (Martin, 2016).

While the technical utility is about the weapon and tactical utility is about the battlefield, strategic utility is about the state. Chapman et al. (2018) interpreted strategic utility as how the use of weapons is in line with objectives, principles, or plans from the national strategy. Besides that, Chapman et al. (2018) also include the rhetoric and actions of individual states as one of the frameworks to examine the strategic utility.

Chapman et al. (2018) who used Martin’s military utility concept to analyze chemical weapons in the Syrian Civil War suggested that the concept is helpful to provide descriptions of what states have more to gain from acquiring or using weapons. This makes the use of the military utility concept as an analytical framework applicable to the research question of this article. Besides that, the qualitative conceptualization of the military utility is also relevant to the method used in this article. Chapman et al. (2018) demonstrated it by operationalizing literature-based studies as the main data collection technique and using contemporary scholarships as the primary data sources in their article.

Technical Utility of Db1000n

Db1000n is a software to launch a Distributed Denial of Service (DDoS) attack against Russia’s information infrastructure. DDoS is defined by Keromytis (2017) as an attack where a huge number of computers are simultaneously seeking access to an online service. It is one of the most common types of attack that can make the target run out of operation and exhaust the intermediate networking path around the target (Gupta & Dahiya, 2021). Many DDoS attack software is already available in the market, such as Mstream, Trinoo, and HOIC (Gupta & Dahiya, 2021). But, db1000n is a DDoS attack software created for Ukraine’s cyber warfare effort specifically.

The creation of db1000n was first initiated by a Ukrainian cyber security specialist named Ivashko (2022c) on February 26, 2022. Since then, a total of 50 contributors have been helping in the development of db1000n up to now (Ivashko, 2022f). Db1000n is developed and maintained by the contributors in the GitHub (2022) repository, one of the leading online platforms that facilitate software project collaboration and management. The software itself has been through several iterations since its creation. Version 0.8.0 was the first to be adopted officially by the Ukrainian IT army, while the newest as of August 9, 2022, is version 0.9.17 (Ivashko, 2022g).

Ivashko (2022d) and contributors used "Go" as the programming language to develop db1000n. Go language was first created at Google by Robert Griesemer, Rob Pike, and Ken Thompson in March 2012 (McGrath, 2020). According to Bodner (2021), the Go language is intended for creating software that will last for a long time and can be modified by huge numbers of computer programmers over many years. With that intention, programming in the Go language lean to be more straightforward and sometimes quite repetitive compared to most programming languages nowadays (Bodner, 2021). But in return, the Go language is fast and simple to write (McGrath, 2020).

Db1000n can be installed and run by anyone who wants to providse their computer as a DDoS attack launch point. The software is supported in several operating systems such as Windows, Linux, and Macintosh (IT Army of Ukraine, 2022b). Based on the instruction manual, someone who wants to join the attack on Russia's information infrastructure needs to do two things, namely download the latest version of db1000n from GitHub and start the software (IT Army of Ukraine, 2022b). The Ukrainian IT army also gave an optional instruction which is to use virtual private networks (VPN) before launching the software. VPN allows a more secure and reliable connection over the internet (Ashraf, 2018).

The following paragraph will describe the way db1000n works. The software regularly fetches files that contain a list of Russia's information infrastructure targets from the Ukrainian IT army's server to the local computer (Ivashko, 2022a). The files arrange what target should be attacked in parallel with other computers that also have db1000n installed on them (Ivashko, 2022a). Db1000n will keep launching DDoS attacks on the arranged target as long as the software and the internet connection run (IT Army of Ukraine, 2022b). In short, db1000n works by managing target change automatically from the Ukrainian IT army's computer to many computers during DDoS attacks against Russia.

The first use of db1000n by the Ukrainian IT army was when attacking four Russian government websites on March 24, 2022. These four websites are the portal of foreign economic information, the ministry of foreign affairs, the ministry of economic development, and the ministry of education and science (IT Army of Ukraine, 2022a). The Ukrainian IT army claimed that the attack was successful to make the websites run out of operation (IT Army of Ukraine, 2022e). As of April 23, 2022, only the ministry of economic development website and the ministry of education and science website had come back into operation (Ministry of Economic Development of Russia, 2022; Ministry of Education and Science of Russia, 2022).

Db1000n was also used by the Ukrainian IT army to attack Russian company websites, for example, an attack was launched against an express delivery service company in Russia named CDEK to disrupt and wipe out its courier system on March 25, 2022 (IT Army of Ukraine, 2022f). The Ukrainian IT army claimed they managed to achieve the goal within seven hours (IT Army of Ukraine, 2022g). Russian media started to pay attention to Ukraine's db1000n after this attack. One of them was the Russian state-owned news agency Novosti (2022) which claimed that the attack caused national-scale failures in CDEK operations for several hours.

As of August 9, 2022, the use of db1000n has been taken down as many as 186 Russian websites (IT Army of Ukraine, 2022j). Most of the websites are Russian government websites and Russian bank websites, for example:

1. Ministry of State Security;
2. Ministry of Revenue and Duties;
3. Donetsk People's Republic Government;
4. Ministry of Culture;
5. Ministry of Construction, Housing, and Public Facility;
6. Gazenergo Bank;

7. Kuznetsk Business Bank;
8. Khakass Municipal Bank;
9. Moscow Industrial Bank; and
10. Child Bank (IT Army of Ukraine, 2022j).

Db1000n is not an entirely perfect software for cyber warfare, despite its success in attacking the Russian government or company websites. A total of 249 issues have been reported since (Ivashko, 2022h) created the software. The most prominent issue is that db10000n sometimes failed to fetch target list files from the Ukrainian IT army's server which caused the computer unable to configure the attack properly (Bondarenko, 2022; Pashagolub, 2022; Chmil, 2022). So far, 189 issues have been solved by db1000n contributors by frequently releasing a new version of the software (Ivashko, 2022e). The remaining 37 issues are still being discussed by the contributors on GitHub up to now (Ivashko, 2022i).

Tactical Utility of Db1000n

Cyber warfare has different characteristics compared to warfare on land, sea, or air. Cyberspace does not have a definable expanse because it exists in multiple locations of many computer systems and networks (Sloan, 2017). But, this does not mean cyberspace as a new domain of warfare has different nature than warfare in other domains because it is still the application of force against the enemy (Sambaluk & Spafford, 2020). This also implies that cyber warfare tactics have the same basic principles as other domains which is the use of forces to win engagements (Echevarria, 2017). The following section will present a further description of the identified tactical utility of db1000n.

The first tactical utility of db1000n it allows an easier way to amass many computers during the attack against the Russian government or company websites. It could be said that DDoS attacks are one of the easiest attacks to launch in cyberspace because these attacks do not need someone to have great cyber security knowledge to inflict damage (Sambaluk & Spafford, 2020). However, one major drawback of DDoS attacks is acquiring a large number of computers as hosts to launch it in the first place (Keromytis, 2017). DDoS attacks according to Gupta & Dahiya (2021) rely heavily on the dispersion of multiple distributed launch points against the target. In other words, the more computers launch DDoS attacks, the more damages are inflicted.

In this matter, db1000n supports Ukraine's cyber warfare effort against Russia by being available to be downloaded openly on the web. All versions of db1000n have been downloaded from GitHub more than 345 thousand times since its creation on the last of February 2022 (Shehryar, 2022). The latest version of the software itself, which was released in the first week of August 2022, has been downloaded around two hundred times now (Shehryar, 2022). Meanwhile, the most downloaded version of db1000n is version 0.7.12 with a total number of downloads as many as 35 thousand times (Shehryar, 2022). This version was the predecessor of version 0.8.0, the first version that was officially adopted by the Ukrainian IT army (Ivashko, 2022b). Further details on the last 18 versions of db1000n can be seen in Table 1.

Table 1. Total Downloads of Db1000n Version 0.9.0 until Version 0.9.17 as of August 9, 2022

Version	Downloads	Version	Downloads
0.9.0	3136	0.9.9	6833
0.9.1	604	0.9.10	8284
0.9.2	1521	0.9.11	6678
0.9.3	15891	0.9.12	406
0.9.4	6643	0.9.13	10055
0.9.5	19828	0.9.14	8
0.9.6	5228	0.9.15	1539
0.9.7	0	0.9.16	176
0.9.8	14800	0.9.17	2264

Source: Shehryar (2022)

The Ukrainian IT army also has acknowledged that the more db1000n downloaded, the more optimal db1000n's tactical utility for cyber warfare against Russia. Some efforts have been done by the Ukrainian IT army to encourage internet users to download the db1000n and keep up to date with the new version of the software. One of the efforts is using their official Telegram channel to remind it online frequently when announcing the result of the DDoS attacks against Russia. For instance, the Ukrainian IT army did it when announcing the result of the attack against the Russian CDEK express delivery service website on March 26, 2022 (IT Army of Ukraine, 2022g).

The second and the last tactical utility of db1000n is helped to counter a new Russia's tactics to ward off Ukraine's DDoS attacks against them. The Ukrainian IT army claimed that the Russian websites started to employ two DDoS attack defense mechanisms on March 23, 2022, called Internet Protocol (IP) address change and IP address block (IT Army of Ukraine, 2022d; IT Army of Ukraine, 2022h). An IP address is a unique identification number that is assigned and configured to each device either manually or automatically to be able to communicate on the internet (Rooney & Dooley, 2021). It serves as the beginning and endpoint of message delivery in two ways communication between many computers on the internet.

The IP address change tactic makes Russian government or company websites become hidden among many computers' IP addresses that are not Ukraine's DDoS attacks targets (IT Army of Ukraine, 2022d). Whereas the IP address block tactic makes Ukraine's DDoS attacks against Russia's information infrastructure would fail even before these attacks are launched because the target self-isolates from the internet for several moments (Gupta & Dahiya, 2021; IT Army of Ukraine, 2022h). The Ukrainian IT army claimed that the implementation of the IP address change tactic and IP address block tactic caused the success rate of DDoS attacks without using db1000n to only 40% as of April 1, 2022 (IT Army of Ukraine, 2022i).

Most of the Russian websites that used both tactics are Russian banks, for instance Cetelem Bank, NK Bank, Kremlin Bank, Tender Bank, and Alternative Bank (IT Army of Ukraine, 2022j). Meanwhile, the Russian government website has been using both tactics for the invasion only by the Ministry of Information (IT Army of Ukraine, 2022j). IT Army of Ukraine (2022j) claimed the IP address change tactic and the IP address block tactic make those five Russian bank websites and the ministry of information website still can be accessed as of August 9, 2022.

In that respect, db1000n helps Ukraine's cyber warfare effort against Russia by target switching automatization. As mentioned in the technical utility section, db1000n has a fetch files mechanism to manage DDoS attack targets from the Ukrainian IT army's server to the local computer. The mechanism allows the Ukrainian IT army to change the target of the DDoS attack instantly for every computer that has db1000n installed and turned on when encountering the IP address change tactic or IP address block tactic by Russia. This is also in line with the target adjustment as an important key to maintaining tactical advantages in cyberspace for the long term. According to Libicki (2021), target adjustment ensures the concentration of force against those that respond slowly regardless of how attacks in cyberspace are employed.

Nevertheless, a DDoS attack using designated computer software like db1000n is not the ultimate tactic in cyber warfare. There are still many types of software that can be operationalized to win military engagement in cyberspace. One of them is called malicious software (malware). This software works primarily by seeking to duplicate themselves from one computer to many computers and then cause some substantial form of damage such as corrupting data and disabling networks (Cares, 2017). According to Cares (2017), malware can be divided into seven main categories, which are computer viruses, worms, trojan horses, spyware, adware, ransomware, and scareware.

Despite that, the tactical utility of DDoS attack software like db1000n is still sufficient compared to malware in the Russian invasion of Ukraine case. Db1000n already overcome the problem of acquiring a large number to launch DDoS attacks based on the download statistics. The automated fetch files mechanism of db1000n also proved relevant to counter the IP address change tactic and IP address block tactic used by the Russian websites.

Strategic Utility of db1000n

Ukraine officially put into force the Strategy of National Security on February 16, 2022. Just around a week before the 2022 Russian Invasion of Ukraine happened. This strategy which is planned to implement by 2025 serves as the foundation for determining the real and potential threats to Ukraine's security,) directions and objectives of Ukraine's security, and planning and implementing Ukraine's security policy (Office of the President of Ukraine, 2022). In general, the Strategy of National Security itself consists of four sections, namely 1) general provisions; 2) security environment and threats to national security; 3) goals, directions, and objectives of national policy on security issue; and 4) organizational and financial support for the strategy implementation (Office of the President of Ukraine, 2022).

The goal of Ukraine’s security based on the strategy is the prevention, detection, and elimination of internal and external threats to national security and the conditions that facilitate the occurrence of those threats (Office of the President of Ukraine, 2022). The strategy stated clearly that the main threat to Ukraine’s security for the next few years is Russia because of their systematic use of political, economic, informational, psychological, and cyberspace means in the ongoing conflict (Office of the President of Ukraine, 2022). Furthermore, the strategy also stated that something is a threat to Ukraine’s security when it is made difficult for Ukraine to protect the national sovereignty, territorial integrity and democratic constitutional order, and other vital national interests (Office of the President of Ukraine, 2022).

The goal stated in Ukraine's Strategy of National Security reflects the survival assumption of the structural realism approach. Pashakhanlou (2016) affirmed structural realism and explicitly said that survival is important for the state since it is the prerequisite for the accomplishment of all other goals in international politics. It bases on the main argument by well-known structural realism thinker Kenneth that states seek to ensure their survival in the anarchical structure of the international system (Waltz, 1979). Additionally, Russia as the main threat to Ukraine's security for the next few years further illustrates how structural realism sees the relations among sovereign states. According to Baylis (2020), structural realism described the durability of anarchical structure in the international system implying that interstate relations in the future are more likely to be violent.

The Strategy of National Security also gave general orientations as the foundation on how Ukraine should deal with the threats. The general orientations consist of twenty-one points that cover counterintelligence to international cooperation (Office of the President of Ukraine, 2022). Three of them gave concerns on military technology and cyber warfare, which are 1) development of national security capabilities system about timely prevention, detection, and countermeassurment of Ukraine's external and internal threats; 2) completion of establishment, development, and reinforcement of the cyber security system capabilities to effectively combat cyber threats in the modern security environment; and 3) increasing the technological capabilities of the national security with the adoption of the latest systems of hardware and tools (Office of the President of

Ukraine, 2022). Refers to Ukraine's security goal and three general orientations that have been mentioned above, the usage of db1000n against Russia is in line with the Strategy of National Security. It can be argued that overall db1000n has strategically relevant utility as a tool to countermeasure and combat Russian threats in cyberspace by boosting Ukraine's technological capability in cyberspace for current circumstances. This strategic utility not only came out of necessity due to the 2022 Russia Invasion of Ukraine happened but also because the db1000n itself has been proven to possess the technical utility and the tactical utility based on the findings and discussion in the two previous sub-sections of this article. In short, the way db1000n works and supports cyber warfare objectives against Russia is well relatable to Ukraine's seeks for survival in the international system. The following section will present further elaboration on this matter.

DDoS software like db1000n is a recent expansion on what tools can be strategically wielded when dealing with other states. According to Kello (2017), this creates two implications that states must consider for their foreign affairs, first, there will be problems with the technology’s sheer speed of action that can make states not fully comprehend and manage them and, second, there will be revolutionary empowerment that can help states to achieve their goals and preserve their national interests in the anarchical structure of the international system. Additionally, Kello (2017) also argued both of the implications will create shock in international order by making the conflict in cyberspace not easy to model, regulate, and terminate among sovereign states. This further complicates the conflictual and uncertain tendency of international politics for states that have been interconnected in cyberspace.

DDoS attacks using software like db1000n make a strategic advantage in current international politics. Buchanan (2020) argued many states have relied on cyber warfare in recent years as a playbook of statecraft to gain advantages over other states by conducting attacks, espionage, or destabilization in cyberspace. Cyber warfare has an accumulation of strategic effects for states because it is one form of covert action with high force, precision targeting, and unexpected timing (Buchanan, 2020). Moreover, the rapid progression of technology also opens up a clear possibility to inflict more damage on targets that cannot be anticipated flawlessly by states over time. According to Buchanan (2020), this pattern has strategic implications for many states because they will embrace it to attack one another as the key part of the struggle for power in cyberspace.

Even though there is a utility to ensuring states' survival in a broad sense, the strategic expectations realization of software like db1000n is still challenging for now. Maschmeyer (2021) found there is a trilemma that limits the strategic utility of many tools for cyber warfare, namely slow operational speed to start to produce meaningful effects, constraint on scope and scale of the effects, and efforts to maintain control over a targeted system. Each part of the trilemma is negatively correlated, which means the state’s gains in one part of the trilemma tend to produce losses across the other two parts (Maschmeyer, 2021). This is why Maschmeyer (2021) concluded that the existence of those trilemma makes strategic expectations of attacks in cyberspace can fall short and only deliver limited utility for the state. Based on Maschmeyer’s trilemma, it could be hypothesized that the use of db1000n faces two problems, namely constraint on the scope and scale of the effects and efforts to maintain control over a targeted system. One piece of evidence that leads to this hypothesis is adopt a new software called “mhDdos" (IT Army of Ukraine, 2022k). This software was created by a cyber security specialist named Oleksandr on June 24, 2022 (Black, 2022).

CONCLUSIONS, RECOMMENDATION, AND LIMITATION

Therefore, how does the use of db1000n help Ukraine against the Russian invasion? This article concludes with the following answer based on the results and discussion in the previous section. The use of db1000n helps Ukraine to gain advantages against the Russian invasion by being technical, tactical, and strategic DDoS attack software. Technical means straightforward cyber warfare software, tactical stands for effectively countering the Russian defense mechanism in cyberspace, and strategic implies ensuring Ukraine's survival in the current conflictual condition. Despite that, db1000n is not the pinnacle of cyber warfare software because it still needs to be maintained properly and does not guarantee easy success.

This article proposes three recommendations based on limitations to fully contribute to the discussion of military technology and cyber warfare. First, further evidence for the military utility of db1000n is needed because the 2022 Russian invasion of Ukraine is still ongoing. Second, a comparative case study is necessary to verify the military utility of db1000n among other DDoS attack software. Last, further research is required to investigate Maschmeyer's trilemma in the strategic utility of db1000n.

REFERENCES

Ashraf, Z. (2018). *Virtual Private Networks in Theory and Practice*. Chisinau: Scholars’ Press.

Baylis, J. (2020). International and Global Security. In J. Baylis, S. Smith, & P. Owens (Eds.), *The Globalization of World Politics*. New York: Oxford University Press.

Black, O. (2022). Ukita Installer. Retrieved July 11, 2022, from https://github.com/OleksandrBlack/ukita_installer/releases/tag/2.0.0

Bodner, J. (2021). *Learning Go: An Idiomatic Approach to Real-World Go Programming*. Sebastopol: Sebastopol.

Bondarenko, A. (2022). Dynamic Targets List. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/issues/85

Brilmayer, L. (1999). Realism Revisited: The Moral Priority of Means and Ends in Anarchy. *Global Justice*, *41*, 192–215.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and New Normal of Geopolitics*. Cambridge: Harvard University Press.

Cares, J. R. (2017). Malware. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare*. California: ABC-CLIO.

Chapman, G., Elbahtimy, H., & Martin, S. B. (2018). The Future of Chemical Weapons: Implications from the Syrian Civil War. *Security Studies*, *27*(4). https://doi.org/10.1080/09636412.2018.1483640

Chmil, Y. (2022). Always Same Targets. Retrieved July 12, 2022, from https://github.com/Arriven/db1000n/issues/132

Choucri, N. (2012). *Cyberpolitics in International Relations*. London: The MIT Press.

Cohen, E. A. (2018). Technology and Warfare. In J. Baylis, J. Wirtz, & C. Gray (Eds.), *Strategy in the Contemporary World*. New York: Oxford University Press. https://doi.org/10.1093/HEPL/9780198807100.001.0001

Dunne, T., & Schmidt, B. (2019). Realism. In J. Baylis, S. Smith, & P. Owens (Eds.), *The Globalization of World Politics: An Introduction to International Relations*. New York: Oxford University Press.

Echevarria, A. J. (2017). Military Strategy: A Very Short Introduction. In *Military Strategy: A Very Short Introduction*. New York: Oxford

University Press. https://doi.org/10.1093/ACTRADE/9780199340132.001.0001

Fedorov, M. (2022). We are Creating an IT Army. Retrieved July 11, 2022, from Twitter website: https://twitter.com/fedorovmykhailo/status/1497642156076511233

GitHub. (2022). GitHub Docs. Retrieved July 11, 2022, from https://docs.github.com/en

Green, J. A. (2015). Introduction. In *Cyber Warfare: A Multidisciplinary Analysis*. New York: Routledge.

Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures*. Boca Ration: CRC Press.

Hughes, T. P. (1994). Technological Momentum. In M. R. Smith & L. Marx (Eds.), *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge: Massachusetts Institute of Technology Press.

IT Army of Ukraine. (2022a). Good Morning! We Return to Work with the Public Sector. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022b). Death by 1000 Needles. Retrieved July 11, 2022, from Telegram website: https://telegra.ph/Death-by-1000-needles-03-17

IT Army of Ukraine. (2022c). Friends, it’s time to combine all our attacks on the information infrastructure of the “Needle” invader. Retrieved July 11, 2022, from Telegram website: https://t.me/s/db1000n

IT Army of Ukraine. (2022d). For the Second Day in a Row, Our Enemy Has a New Tactic to Counter our Attacks, Namely, Changing IP Addresses. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022e). A Bit of Feedback on The State of Our Affairs. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022f). Good Morning! Attacks on Delivery Services Have a Very Tangible Result. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022g). Good Morning, IT Army! Thanks to Our Coordinated Actions. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022h). Good Morning! It is Becoming Increasingly Difficult to Carry out Attacks. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022i). A Bit of sSatistics. So Far, Only 40% of Our Targets Have Been Sent Out. Retrieved July 11, 2022, from Telegram website: https://t.me/s/itarmyofukraine2022

IT Army of Ukraine. (2022j). Information about Current Targets Status. Retrieved August 11, 2022, from https://itarmy.com.ua/check/?lang=en

IT Army of Ukraine. (2022k). Instructions for Setting up DDOS Attacks. Retrieved August 11, 2022, from https://itarmy.com.ua/instruction/?lang=en

Ivashko, B. (2022a). Death by 1000 Needles. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/blob/main/README.md

Ivashko, B. (2022b). v0.7.12. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/releases/tag/v0.7.12

Ivashko, B. (2022c). Contributors: Feb 20, 2022-Feb 26, 2022. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/

graphs/contributors?from=2022-02-20&to=2022-02-26&type=c

Ivashko, B. (2022d). 43 Code Results in Arriven/db1000n. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/search?l=go

Ivashko, B. (2022e). Closed Issue. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/issues?q=is%3Aissue+is%3Aclosed

Ivashko, B. (2022f). Contributors: Feb 20, 2022 -Apr 23, 2022. Retrieved July 11, 2022, from https://github.com/Arriven/db1000n/graphs/contributors?from=2022-02-20&to=2022-04-05&type=c

Ivashko, B. (2022g). db1000n v0.8.29. Retrieved August 11, 2022, from https://github.com/arriven/db1000n/releases/tag/v0.9.17

Ivashko, B. (2022h). Issues. Retrieved August 11, 2022, from https://github.com/Arriven/db1000n/issues?q=is%3Aissue

Ivashko, B. (2022i). Open Issue. Retrieved August 11, 2022, from https://github.com/Arriven/db1000n/issues?q=is%3Aopen+is%3Aissue

Kello, L. (2017). The Virtual Weapon and International Order. In *The Virtual Weapon and International Order*. New Haven: Yale University Press. https://doi.org/10.2307/J.CTT1TRKJD1

Keromytis, A. D. (2017). Distributed Denial of Service (DDoS) Attack. In P. J. Springer (Ed.), *Encyclopedia of Cyber Warfare* (pp. 91–93). Santa Barbara: ABC-CLIO.

Libicki, M. C. (2021). *Cyberspace in Peace and War*. Annapolis: Naval Institute Press.

Lucas, G. (2016). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. In *Ethics and Cyber Warfare*. New York: Oxford University Press. https://doi.org/10.1093/ACPROF:OSO/9780190276522.001.0001

Martin, S. B. (2002). The Role of Biological Weapons in International Politics: The Real Military Revolution. *Journal of Strategic Studies*, *25*(1), 63–98. https://doi.org/10.1080/714004040

Martin, Susan B. (2004). Realism and Weapons of Mass Destruction: A Consequentialist Analysis. In S. H. Hashmi & S. P. Lee (Eds.), *Ethics and Weapons of Mass Destruction: Religious and Secular Perspectives*. New York: Cambridge University Press.

Martin, Susan B. (2013). The Continuing Value of Nuclear Weapons: A Structural Realist Analysis. *Contemporary Security Policy*, *34*(1), 174–194. https://doi.org/10.1080/13523260.2013.771042

Martin, Susan B. (2016). Norms, Military Utility, and the Use/Non-use of Weapons: The Case of Anti-plant and Irritant Agents in the Vietnam War. *Journal of Strategic Studies*, *39*(3), 321–364. https://doi.org/10.1080/01402390.2016.1181058

Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations. *International Security*, *46*(2), 51–90. https://doi.org/10.1162/ISEC_A_00418

McGrath, M. (2020). *Go Programming in Easy Steps: Learn Coding with Google's Go Language*. London: Easy Steps Limited.

Ministry of Economic Development of Russia. (2022, April 23). About. Retrieved July 11, 2022, from https://www.economy.gov.ru/material/structure/

Ministry of Education and Science of Russia. (2022). About. Retrieved July 11, 2022, from https://minobrnauki.gov.ru/about/governance/

Mori, S. (2018). US Defense Innovation

and Artificial Intelligence. *Asia-Pacific Review*, *25*(2), 16–44. https://doi.org/10.1080/13439006.2018.1545488

Mori, S. (2019). US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-PasificReview*, *26*(1), 77–120. https://doi.org/10.1080/13439006.2019.1622871

Novosti, R. (2022). В работе сервиса СДЭК произошел глобальный сбой. Retrieved April 17, 2022, from https://ria.ru/20220325/sdek-1780037937.html

Office of the President of Ukraine. (2022). Decree of The President of Ukraine No. 56/2022. Retrieved July 12, 2022, from https://www.president.gov.ua/documents/562022-41377

Pashagolub. (2022). Failed to Fetch Config. Retrieved May 13, 2022, from https://github.com/Arriven/db1000n/issues/217

Pashakhanlou, A. H. (2016). *Realism and Fear in International Relations: Morgenthau, Waltz and Mearsheimer Reconsidered*. New York: Palgrave MacMillan.

Roland, A. (2016). *War and Technology: A Very Short Introduction*. New York: Oxford University Press.

Rooney, T., & Dooley, M. (2021). *IP Address Management*. Hoboken: John Wiley & Sons.

Sambaluk, N. M., & Spafford, E. H. (2020). *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*. Santa Barbara: ABC-CLIO.

Schneider, J. (2019). The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and The Onset of War. *Journal of Strategic Studies*, *42*(6), 841–863. https://doi.org/10.1080/01402390.2019.1627209

Shandler, R., Gross, M. L., & Canetti, D. (2021). A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in The United States, United Kingdom, and Israel. *Journal Contemporary Security Policy*, *42*(2), 135. https://doi.org/10.1080/13523260.2020.1868836

Shehryar. (2022, August 9). Arriven db1000n. Retrieved August 12, 2022, from https://hanadigital.github.io/grev/?user=Arriven&repo=db1000n

Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *Journal The International Spectator*, *53*(2), 111–123. https://doi.org/10.1080/03932729.2018.1453583

Sloan, E. C. (2017). *Modern Military Strategy: An Introduction*. New York: Routledge.

Thornton, R., & Miron, M. (2020). Towards the ‘Third Revolution in Military Affairs’: The Russian Military’s Use of AI-Enabled Cyber Warfare. *The RUSI Journal*, *165*(3), 12–21. https://doi.org/10.1080/03071847.2020.1765514

Tidy, J. (, February). Russian Vigilante Hacker: “I Want to Help Beat Ukraine from My Computer.” Retrieved May 17, 2022, from https://www.bbc.com/news/technology-60528594

Waltz, K. N. (1979). *Theory of International Politics*. Philippines: Addison-Wesley Publishing Company.

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods*. London: SAGE Publications.