Vol. 10, No. 4, 2024, pp. 16-21
DOI: https://doi.org/10.29210/020243157

Contents lists available at Journal IICET

JPPI (Jurnal Penelitian Pendidikan Indonesia)
ISSN: 2502-8103 (Print) ISSN: 2477-8524 (Electronic)

Journal homepage: https://jurnal.iicet.org/index.php/jppi

Russia vs America cyber war: space technology mastery competition

Fadra Fadra[1*)], Joseph Teguh Santoso[2]
[1] Faculty of Social and Political Sciences, University of Prof. Dr. Moestopo (Beragama), Jakarta, Indonesia
[2] Universitas STEKOM, Semarang, Jawa Tengah, Indonesia

Article Info

Article history:

Received Aug 10th, 2023
Revised Oct 15th, 2023
Accepted Oct 08th, 2024

Keyword:

NATO,
Cyber Warfare,
Space technology hegemony,
Great power politics,
Cyber attack

ABSTRACT

Mastery of computers and information systems in international relations is one of the elements of a country's new power. In the context of cyber warfare, Russia and the United States are trying to modernize their technology to secure their countries in the event of an attack from the opposing party. This research aims to analyze the space technology competition carried out by two major countries, namely Russia and the United States, to achieve Great Power status in the international world. This research focuses on the technological achievements of Russia and the United States in the field of space and their implementation in the form of cyber warfare. A qualitative case study is the research method chosen by the researcher. The research stages used by researchers are divided into data collection stages and data reduction, and the next stage is that researchers conduct analysis using data reduction techniques, namely summarizing, selecting, and focusing on the things needed in this study. The results of this study show that national security priorities are number one, and especially defense priorities for the United States are no longer terrorism but great power competition. NATO is an alliance or political tool that the US relies on to achieve great power.

Corresponding Author:

Fadra Fadra
University of Prof. Dr. Moestopo (Beragama), Jakarta
Email: fadra@dsn.moestopo.ac.id

Introduction

The development of science in the field of space exploration made it possible to immediately realize the predictions of Arthur C. Clarke. Research on the possibility of using artificial Earth satellites as radio repeaters began already in the second half of the 1950s. Soviet scientists managed to take them out of the theoretical field into the practical field. On October 4, 1957, the world's first artificial Earth satellite was launched by the Soviet Union. He not only marked the beginning of the space era but also laid the foundation for satellite communications. It was the first object in space to have its signal received on Earth. In the 1960s, the next passive satellite was launched by the US. Since then, satellite communications have continued to evolve, which means more and more satellites are launched into orbit every year. Today, a total of about 8 thousand satellites revolves around the Earth (Roscosmos, 2022).

Cybernetics is the science of the general principles of control in various systems: technical, biological, social, and others (Novikov, 2015). Control is a central concept of cybernetics. Each phase of the control/management process takes place in interaction with the environment. Therefore, in cybernetics, much attention is paid to the study of feedback and the concept of the "black box". While Informatics emerged due to the development of

computer technology, working inside and impossible without computers. Computer technology acts as a means of processing information for informatics (Lissack, 2021). It can be argued that cybernetics and computer science differ in accent emphasis. If the information properties and processing systems of the device (hardware or soft) are in a computer, then in cybernetics the emphasis is on the development of concepts and construction of control models. And both are inseparable from the function of satellites.

With the advancement of satellite technology into a new strategy in the concept of *Great Power*, this is starting to become a major concern for international relations policymakers. From financial losses to businesses through cybercrime, theft of confidential government data, or targeting critical infrastructure, cybersecurity poses significant challenges to countries' economic and national security globally. Cyberspace is now considered the fifth warfare domain after land, sea, air, and space (Economist 2010), and traditional frameworks can help us understand this relatively new form of conflict (Craig & Valeriano, 2018). Although we can see the actual hardware (computers, routers, wires), their interactions take place in an invisible digital world. This allows for assaults against public or private sector institutions in one region of the world to be launched from another region. Cybercrime, cyberespionage, and cyberattack are all terms that are frequently used interchangeably with one another. We speak about hackers, cybercriminals, and cyberterrorists as if they were identical. It's possible, or at least likely, that they're related in many situations. There have been many distinct definitions of cyberwar. Cyberwar has frequently been conceptualized within the framework of traditional concepts of warfare, as war is generally understood to be a military endeavor. These notions generally involve force, physical harm, and violence.

It is practically impossible to recognize every cyberattack that occurs. Some of them can stay hidden for years. Some are fleeting, but they don't leave a trace either. The space backbone of the information grid, where space as sets are the deciding element, is the central component in the creation of global war-fighting capabilities. When it comes to national security, the United States currently depends on a small number of widely utilized satellites in space. Critical to strategic deterrence, surveillance, information gathering, and military communications, these satellites are an absolute necessity. The satellites play a crucial role in offensive and defensive ballistic missile defense if strategic deterrence fails. Information superiority, the driving force behind the successful multichannel joint war-fighting machinery of recent conflicts, relies heavily on satellites. American military can battle globally be cause of access to satellite-supported C4ISR. All potential enemies, regardless of size or motive, are aware that the US military's might is intrinsically tied to the capabilities of US space assets (Kallberg, 2012; Merrin, 2018).

As long as the United States maintains space superiority, a small number of states that view themselves as geopolitical actors will be forced to abide by norms they did not help craft. It is unsettling to authoritarian governments that the United States uses its space assets to keep tabs on their activities and their quest for regional dominance. As a result, any reduction or restriction of American space-based capabilities would be celebrated by authoritarian governments. Indirectly or directly, these adversary actors can harm US space assets through cyberwarfare with little to no risk of attribution or traceability (James Moltz, 2011; James Clay Moltz, 2019). Alongside the United States, one non-Western country with strong cyber might is Russia, Russia is the only government to have launched cyber power strikes against other countries, and to date, only Russia has demonstrated the ability to successfully integrate INFOOPS with conventional military operations in a real conflict against nation-states. Russia employs CNO heavily against countries it considers to be in its sphere of influence (former Soviet Union members), using it as a supplement to energy diplomacy, secret service activities, financial and diplomatic support for unstable governments, military presence, etc (Nagy, 2012).

This article discusses how Russia and the United States are trying to modernize their technology to secure their countries in the event of an attack from an opposing party. The purpose of this research is to analyze the space technology competition carried out by two major countries, namely Russia and the United States, to achieve Great Power status in the international world. This research focuses on the technological achievements of Russia and the United States in the field of space and its implementation in the form of cyber warfare.

Method

A qualitative case study is the research method the researcher has chosen. According to Sugiyono (2019), qualitative research methods are often called naturalistic research methods because the research is conducted in natural conditions. Researchers chose this because it was considered appropriate. In addition, researchers want to know about the technological achievements of Russia and the United States in the space field and their implementation in the form of cyber warfare. Researchers analyzed the data by observing, identifying, and explaining in depth the results of the research. The data collection technique that researchers use is based on existing observation and documentation data (Creswell & Creswell, 2017). The research stages used by

researchers are divided into data collection stages, where researchers conducting this research collect data; data reduction, when all data is collected; and the next stage is for researchers to analyze using data reduction techniques, namely summarizing, selecting, and focusing on the things needed in this study.

Results and Discussions

Mastery of Russian Space Technology

On October 6, 1957, Soviet newspapers reported: "The first Soviet-made Earth satellite successfully launched". And all the newspapers in the world carry this. In November 1957, on the second satellite, a dog named Laika went into space, becoming the "first living astronaut" on Earth. On December 6, 1957, in a festive atmosphere with a large crowd at Cape Canaveral, the launch of the first American satellite would take place. (Culture, 2018) Millions of Americans watched on live TV screens, but the rocket was only able to climb 1.2 m, after which it tilted and exploded. On April 12, 1961, Yuri Gagarin became the first human to go into space for 1 hour and 48 minutes to circumnavigate the planet (Culture.ru, 2022).

Alan Shepard became the second man in space after four weeks. But his 15-minute suborbital flight was disappointing compared to Yuri Gagarin's. During the 1960s, Russia developed many satellites and space technology experiments. Of course, in the process, it does not close the many tragedies of astronaut deaths due to landing failures. America that year was busy preparing for lunar flight experiments, one of which was on July 20, 1969, Apollo-11 landed on the Moon Satellite with the first astronaut Neil Armstrong. At that time Russia should be preparing for the construction of the space station "Mir", which can be used for astronauts to research and rest. In February 1986, the Orbital complex "Mir" was successfully launched into orbit and functioned until March 23, 2001 (Culture.ru, 2022).

Now the era of the International Space Station (ISS) has been created. ISS is an international joint project, in which, in addition to Russia, there are 13 countries: Belgium, Brazil, Germany, Denmark, Spain, Italy, Canada, Netherlands, Norway, USA, France, Switzerland, Sweden, and Japan. Russia is currently very active in the ISS program, sharing its experience and knowledge for the development of space systems. Until 2011, The only way to get to the station was with a capsule "Soyuz" mounted on its top R-7 missiles that were better than the version that Sergey Korolev designed half a century ago.

One of the largest developers and manufacturers of such devices in Russia is the Ruselectronics holding of Rostec State Corporation. Today it unites legendary companies in the industry: Fryazino Istok, Moscow State Plant and NPP Pulsar, and Saratov Almaz. The products of this company were completed, in particular the communication satellites Molniya-1, Molniya-2, Horizont, Raduga, Globus-1 and Globus-1M, Luch, Hals, "Celina", "Express", "Meridian" and others. (Rostec.ru, 2022) The greater the number and qualifications of satellite technology, the greater the mastery of information. The greater the mastery of information and information management, the more strategic a country becomes a *Great Power*.

Mastery of U.S. Space Technology and NATO Cyber Strategy

Space is increasingly important to the security and prosperity of the Alliance and the Allies. Space capabilities bring benefits in areas – from weather, environmental and agricultural monitoring, to transportation, science, communications, and banking. Cyber threats are currently considered a top national security concern as governments warn against attacks on vulnerable critical infrastructure. In 2012, for example, the then US Secretary of Defense warned about cyberspace 'Pearl Harbor' against the power grid or financial system, both of which rely on computer networks for their operations (Bumiller & Shanker, 2011). According to a 2016 survey, 73 percent of Americans believe cyberterrorism presents a 'critical threat' to the United States (Craig & Valeriano, 2018).

In 2019, the Allies adopted NATO's Space Policy and recognized space as a new operational domain, alongside air, land, sea, and cyberspace. This policy guides NATO's approach to space and ensures appropriate space-based support for the Alliance's operations and missions in areas such as communications, navigation, and intelligence. NATO decided to allocate €1 billion for satellite communications over the next 15 years (Rynning, 2019). In 2020, a memorandum of understanding between Italy, France, the United Kingdom, and the United States agreed to create the most important satellite communications service by 2035. Based on the document, these countries pledged to give the alliance the space potential of their military satellite communications (SATCOM). (Korenev & Howley, 2022) Agree with Korenov's opinion, that NATO wants to maintain leadership in this area, because currently of the approximately 3, 000 satellites in earth orbit, more than half of them are located in NATO member states, including the companies that fund them (Antoni, Giannopapa, & Adriaensen, 2020; Evgeniy Korenev, 2022; Lueschow & Pelaez, 2020).

NATO's Strategic Concept 2022 reaffirms concerns previously expressed by the Allies about increasing threats in space with the presence of space technology in developing nations. (NATO, 2022) According to

Andrey Belousov, Head of Russia's representative at the UN and other organizations in Geneva, the West is seeking to conduct a full audit of all the foundations of international space law. The United States promotes a concept in which space becomes a new combat environment. NATO 2022 notes the desire to extend the effect of Article 5 of the NATO Treaty into space (Evgeniy Korenev, 2022). One of the points in the NATO treaty states that NATO does not seek to become an autonomous space player, but will complement the work of allies, interacting with other international organizations if necessary. At this point, it is clear that NATO wants to expand its hegemony into space, including the mastery of information systems, intelligence needs, control of satellites, and information technology intervention through the satellites of alliance countries. NATO has the potential to be even more supranational than the United Nations Organization.

According to a professor of Saratov National Research University, Evgeny Korenev said that this agreement will threaten Russia and its allies with its implementation. One of the main threats of NATO in space is associated with the development of anti-cosmic and anti-Satellites of several countries. It was noted that Russia and the PRC have achieved the greatest success in this regard, and Iran, as well as North Korea and other countries, began to develop similar potential (Evgeniy Korenev, 2022). Space Mastery means talking about creating a wide range of possibilities from non-internal (blinding and disrupting cosmic agents) to kinetic destructive systems (anti-Satellite missiles in orbit, lasers, and so on). Some threats, such as signal defeats and cyberattacks, potentially originate from non-state actors, including terrorist organizations. The state intelligence information system will be more open to state hegemony, state secrets will be able to become public consumption, and the state will be more vulnerable to new threats. The world's information systems and technology are becoming determinants or new powers in international relations. It is also a new form of so-called *Offensive* and *Defensive Security,* a new transformation of Waltz's theory.

Russian-American Forms of Cyber Warfare in The International

In 2022, international politics is focused on the Ukraine-Russia war (Demir, 2022). The political conflict between these two countries ended in a war that was quite complex and global because it attracted many interests of countries and international organizations. This war is nothing but a continuation of the political misalignment between Russia, the US, and NATO. Russia and the U.S. have traded accusations about cyberattacks. Both are masters of superior space technology, so the use of satellites as a digital warfare strategy is very large. Andrei Krutskikh, a leading cyber expert at Russia's foreign ministry, told Kommersant newspaper that the United States is suspected of carrying out computer attacks against Russia and its allies through its IT Army in Ukraine. On many occasions, the US has mentioned that Russia interfered in the 2008 and 2020 elections in the US through *cyber attacks*. On Ukraine, Biden accused Russia of "malicious cyber activity" against Ukraine, including attacks on commercial satellite communications networks that damaged systems in other European countries (Hansel, 2023; Ignatius, 2022).

The cyber war between Russia and the US is unlikely to end, neither will sit on a single agreement on curbing cyber attacks. The political interests of the two differ, as Eric Chabrow writes that Russia wants an international treaty that goes along with chemical weapons negotiations, prohibits a country from secretly embedding malicious codes or circuits that can later be activated remotely in the event of war, implements humanitarian law prohibiting attacks on noncombatants and prohibits fraud in cyber operations. Russia is demanding international agencies to oversee internet crime. The US argues that an agreement is not needed, as it would not be effective. The U.S. rejects treaties that allow governments to censor the Internet, because it's impossible to know Internet attacks are coming from governments, hackers loyal to the government, or criminals acting independently (Chabrow, 2009; Shuya, 2018; Smith, 2019).

Glenn S. Gerstell, senior adviser at the Center for Strategic and International Studies and former general counsel of the National Security Agency, said Russia was behind the cyber attacks in Ukraine. Russia is recognized as a cyber ruling country, this is evident from what the Soviet Union did related to the SolarWinds attack, the Colonial Pipeline hack, and several ransomware attacks in every industry in the United States (Paul, 2022; Stoddart, 2022). The U.S. currently has tremendous offensive military capabilities to respond at the cyber level, but it has not been able to anticipate cyberattacks or take defensive action. The private sector is unprepared for this kind of attack. From Gerstell's statement, we can conclude that the US recognizes Russia's superiority in the cyber field, but from a political point of view, this statement can also mean provocations or propaganda that the US accuses Russia of which are not necessarily proven.

The problem is that international reporting is also a form of mastery of the mass media, a form of propaganda in shaping a common view. Intensive propaganda can even form false facts. Coverage in the mass media greatly affects the floating mass, developing world countries that cannot reach communication technology. The opinion of international actors will be formed and can become a policy that will influence the policies of other actors. Related to media, mass information, and computers we know the concept of *cyber sabotage,* where the operation is used to suppress or intervene politically. *Cyber sabotage* can be done by the state to withhold certain news, shut

down good or bad news of something, or by cutting off access to media or information. (IISS, 2022) In the first month of Russia's military operation into Ukraine, several official Russian news media sites were inaccessible, such as Russian Today, Ria Novosti, Vedomosti, and Gazeta.ru. Propaganda about support for Ukraine appeared for a few seconds even in the middle of children's content videos on Youtube. Some apps on the play store show flashes of support for Ukraine.

Conclusions

The Internet is not limited by sovereign boundaries. Sometimes hacking is destructive, while other times adversaries enter networks and violate privacy, stealing secrets and data without causing physical damage that is considered equivalent to a physical attack by a bomb or missile. The national security priority being number one and foremost the defense priority for the United States is no longer terrorism, but rather great power competition. NATO became an alliance or political tool that the US relied on in achieving the Great Power. Space projects are not cheap, so countries collaborate for their national security guarantees at a shared cost.

References

Antoni, Ntorina, Giannopapa, Christina, & Adriaensen, Maarten. (2020). Space and Security Programs in the Largest European Countries. *Handbook of Space Security*, *2*(2), 1225–1263.

Bumiller, Elisabeth, & Shanker, Thom. (2011). War evolves with drones, some tiny as bugs. *The New York Times*, *19*.

Chabrow, Eric. (2009). Cyber Cold War: U.S. Vs. Russia. Retrieved from govinfosecurity website: https://www.govinfosecurity.com/blogs/cyber-cold-war-us-vs-russia-p-227

Craig, A. J., & Valeriano, Brandon. (2018). Realism and cyber conflict: Security in the digital age. *Realism in Practice*, *85*(3), 1–11.

Creswell, John W., & Creswell, J. David. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Culture.ru. (2022). Space Race. Retrieved November 16, 2022, from culture.ru website: https://www.culture.ru/materials/50445/kosmicheskaya-gonka

Culture, Ministry of Chuvash. (2018). History of space exploration. Retrieved November 16, 2022, from culture.cap.ru website: https://culture.cap.ru/action/activity/sobitiya/novogodnie-meropriyatiya-v-chuvashskoj-respublike/denj-kosmonavtiki/istoriya-osvoeniya-kosmosa

Demir, Sertif. (2022). The 2022 Russia-Ukraine war: reasons and impacts. *Bölgesel Araştırmalar Dergisi*, *6*(1), 13–40.

Evgeniy Korenev. (2022). NATO Space Strategy: Implications for Russia and its Allies. *Eurasia Expert*. Retrieved from https://eurasia.expert/kosmicheskaya-strategiya-nato-posledstviya-dlya-rossii-i-ee-soyuznikov/

Hansel, Mischa. (2023). Great power narratives on the challenges of cyber norm building. *Policy Design and Practice*, *6*(2), 182–197.

Ignatius, David. (2022). Opinion | The U.S.-Russia conflict is heating up — in cyberspace. Retrieved from washingtonpost website: https://www.washingtonpost.com/opinions/2022/06/07/us-russia-conflict-is-heating-up-cyberspace/

Kallberg, Jan. (2012). Designer satellite collisions from covert cyber war. *Strategic Studies Quarterly*, *6*(1), 124–136.

Lissack, Michael. (2021). Cybernetics and Control. In *Handbook of Systems Sciences* (pp. 87–106). Springer.

Lueschow, Holger, & Pelaez, Roberto. (2020). Satellite Communication for Security and Defense. *Handbook of Space Security: Policies, Applications and Programs*, 779–796.

Merrin, William. (2018). *Digital war: A critical introduction*. Routledge.

Moltz, James. (2011). *The politics of space security: strategic restraint and the pursuit of national interests*. Stanford University Press.

Moltz, James Clay. (2019). The changing dynamics of twenty-first-century space power. *Journal of Strategic Security*, *12*(1), 15–43.

Nagy, Viktor. (2012). The geostrategic stuggle in cyberspace between the United States, China, and Russia. *AARMS*, *11*(1), 13–26.

Novikov, Dmitriĭ Aleksandrovich. (2015). *Cybernetics: from past to future* (Vol. 47). Springer.

Paul, Kari. (2022). 'We are not ready': a cyber expert on US vulnerability to a Russian attack. Retrieved November 16, 2022, from theguardian website: https://www.theguardian.com/technology/2022/mar/10/us-russia-cyber-attack-prepared

Roscosmos. (2022). How it works. Satellite connection. Retrieved November 18, 2022, from Rostec.ru website: https://rostec.ru/news/kak-eto-rabotaet-sputnikovaya-svyaz/

Rynning, Sten. (2019). *NATO's futures: The Atlantic Alliance between power and purpose*. NATO Defense College.
Shuya, Mason. (2018). Russian cyber aggression and the new Cold War. *Journal of Strategic Security*, *11*(1), 1–18.
Smith, Nicholas Ross. (2019). *A new cold war?: Assessing the current US-Russia relationship*. Springer.
Stoddart, Kristan. (2022). Cyberwar: Attacking Critical Infrastructure. In *Cyberwarfare: Threats to Critical Infrastructure* (pp. 147–225). Springer.
Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung : Alphabeta.