DOI: 10.53477/2971-8813-22-53

RECONSIDERING THE CONCEPT OF CHOKEPOINTS FOR THE 21st CENTURY

Mihai VLAICU
MA Student, The National University of Political Studies and Public Administration,
Security and Diplomacy, Bucharest, Romania
vlaicumihai10@gmail.com

Abstract: *Chokepoints can be best described as areas where the ability to transport or deploy assets or goods can be severely denied or restricted, due to their limited spatial characteristics. As such, a potential party to an armed conflict can deploy a relatively small detachment of assets in order to interdict the aforementioned actions, with considerable results, especially during a conventional, large scale war, representing, from a certain perspective, a method of conventional asymmetric warfare against a numerically superior force. During history, chokepoints have been mainly considered to be areas of water or land, where the ability to maneuver of the deployed forces have been severely hindered, although, with the emergence of new warfighting domains, such as cyber and space, the definition of the chokepoint, as well as the perception of using them during warfare, can be expanded. The purpose of this paper is to analyze the different types of non-traditional chokepoints (space and information centered), their origins and vulnerabilities, as well as presenting a series of recommendations with the purpose of increasing their level of security. The methodology of research used in this paper is the historical analysis of the concept of chokepoint, the observation of technical measures that could create to the establishment of new types of chokepoints, as well as that of possible ways of mitigating these security threats.*

Keywords: *Chokepoint; Space launch vehicle; Space vehicle launch facility; Space warfare; Submarine cables; Manned-unmanned teaming.*

Introduction

Chokepoints are generally defined by their geographical characteristics. The maritime chokepoints have as particularity the fact that they are areas through which a combatant has to pass in order to deploy its maritime assets from one body of water to another, areas which are defined by the constraints they pose to maritime navigation, such as shallow or narrow waters.

From a military standpoint, chokepoints can also be described as areas that can be used by a numerically inferior combatant to inflict a disproportionate amount of damage in human lives and resources to a stronger foe, being, thus, a form of asymmetric warfare. Even though most of the chokepoints are usually interpreted as static points that could be used to hamper or neutralize naval activities, the evolution of human societies have led to the development of alternative war-fighting domains, most notably space and information warfare, domains which could create new, prospective chokepoints with effects on the course of actions of future combatants.

1. Space domain-related chokepoints

The development of space technologies from the 1940s have been one centered both on exploration and on military purposes. Although, in the last decades, technologies like the Global Positioning System or solar panels, developed for spacefaring purposes and adapted to terrestrial usage (NASA 2019) (Hsu 2008) have become more common, influencing the daily lives of billions of people, the next generation of space technologies, like reusable launch systems or directed energy systems can prove to have an even bigger impact on defense issues.

The reestablishment of the United States Space Command (Erwin 2019), the creation of the United States Space Force (David 2019), the emergence of similar structures in the military structures of the other permanent members of the United Nations Security Council (Chuter 2020)

(Ni and Gill 2019) (Weitering 2019) (Bodner 2018) and the signing by President Trump of the Executive Order on Encouraging International Support for the Recovery and Use of Space (United States, Executive Office of the President [Donald J. Trump] 2020), can lead to the conclusion that the present great power competition has moved beyond Earth's boundaries.

The economic resources held by the outer space are substantial and could overly change the global balance of power and therefore, as a consequence of this existent possibility, multiple nations started programs for the exploration and, most importantly, the exploitation of this type of resources. For example, a single asteroid is projected to contain more metals than the entire global reserve of metal (Ruiz Leotaud 2021) and the moon Titan being projected of having larger reserves of hydrocarbons than those on Earth (Agency 2008) triggering countries in taking mainly two courses of action, either in favor of developing space exploitation programs (such as the United States) (Ji, Cerny and Piliero 2020) or space warfare programs (such as Russia) (Palkowsky 2021).

The prospective evolution of the industry, in areas such as spacecraft, manned or unmanned, or reusable launch vehicles, leads to little doubt about the fact that these systems can and be used in a dual-purpose capacity in a future conflict in or above Earth's orbit. However, for these vehicles to reach space, they still must be launched from Earth, fact that generates a vulnerability in the entire space system, a very real „chokepoint". Most of the present day launching facilities are defined by two geographical coordinates, the first being their proximity to large bodies of water and the second being their tendency to be near Earth's Equator. The former characteristic is generated by two requirements:

- Launches need to be aborted in a safe manner, locations near bodies of water being ideal for the low probability of re-entry in populated areas;
- A great level of transportability has to be achieved in order to deliver the components of the launch systems.

The latter requirement is defined by physics, as an object being launched nearer to the Equator can use Earth's rotational speed in order to achieve escape velocity quicker and with less fuel, thus increasing the payload delivered in orbit (Doocy 2011). It should be mentioned that the majority of US-aligned countries operate facilities with geographical characteristics like those described before, whilst the Russian and Chinese space agencies or contractors use space-launch inland facilities. The positioning on the map of the main space launch facilities (Greshko 2018) presents the fact that they are modern-day chokepoints, the main national space agencies having to conduct their launches in these places in order to benefit from the above-mentioned advantages for their space delivery systems. In the same time, the locations of these centers illustrate a clear vulnerability to naval or air strikes, or to amphibious operations.

The usage of platform ships for recovering space delivery systems by two of the main commercial space-oriented organizations in the United States, Blue Origin and SpaceX only slightly ameliorates the situation through the advantage that they are mobile, this solution still presenting all of the above-mentioned vulnerabilities. Through their military and commercial relevance, space related infrastructure will tend to grow in importance and become even more of a potential target for future hostile military or paramilitary organizations.

2. Information domain-related chokepoints

The enabling element which led to the increased efficiency regarding the conduct of both military operations and commercial development since the end of the Cold War was the development of the domain of information technologies, the requirements of ever-increasing processing power and speed of data transmission representing constants of the current global security and economy systems. In any industry, while the processing infrastructure is important, the transport and delivery infrastructure represents the element that enables it to have far-reaching and permanent effects, in this case being represented mainly by space-based communications and underwater sea cables.

Whilst the former can very easily be neutralized with anti-satellite missiles (in the case of the systems already deployed in orbit) or through the above-mentioned elimination of the systems required for the delivery of replacement satellites, the latter can be destroyed only through the action of maritime forces.

Even though destroying underwater sea cables could lead to the loss of more than 90% of Internet data used daily worldwide (Gray 2016), thus leading to substantial economic losses both to the aggressors and to the target country/countries, this fact could be overlooked by a military-centric government because the temporary, global loss of communications can be interpreted as a window of opportunity to be used by the aggressor states in creating a new status-quo on a global scale.

One of the states that could use this method of warfare is the Russian Federation, the Russian Navy developing or having in inventory a substantial number of both underwater and surface vessels that could be used for this kind of missions, such as the Project 22010 class intelligence ships (Peter 2018) or the Klavesin (NavalDrones n.d.), and Status-6 (NAVALTODAY.COM 2018) classes of Unmanned Underwater Vehicles.

Also to be taken into account, there are the Russian attempts to build and maintain a national internet network (Wakefield 2019), reducing the level of connectivity of this country with the outside world, and thus preparing itself for such a scenario, action which could be imitated by China (Kharpaol 2019).

However, the geostrategic implications of such an undertaking would be considerable, even for a country such as the Russian Federation, its standing army lacking the servicemen required to be deployed in such large numbers simultaneously in multiple parts of the globe.

This fact could be addressed by the involvement of other countries interested in changing the current global system, with the same or greater access to resources for this kind of action, countries like China, Pakistan, Venezuela or even Turkey representing potential candidates for the scale of this kind of operation.

Also, the substantial number of cables to be cut might simply prove overwhelming even for the considerable human resources like those countries' maritime services have at their disposal, this fact leading to the conclusion that such an action would, most likely, have to involve a large number of underwater unmanned vehicles. This action might take place with an autonomous control system, which would have as objective the successive or simultaneous cutting of the sea cables or self-destructing near the objectives in order to achieve the required level of coordination for maintaining the element of surprise.

An additional element that would have to be addressed in the planning of this kind of operation would be the destruction of the cable-laying vessels and, additionally, the supporting infrastructure for this kind of network. Locating the underwater sea cables on a map (TeleGeography n.d.) could lead to the conclusion that most of them are grouped relatively together, these groupings representing chokepoints, each with a high degree of vulnerability to an attack such as the one presented above.

3. Recommendations

Both types of infrastructure described (space and information) are vulnerable to attack by maritime assets, mainly by underwater vehicles, through the usage of cruise missile or unmanned vehicle swarms.

At this moment, the best course of action is represented by the development of systems based on the Manned-Unmanned Teaming (Iriarte 2016) principle, particular emphasis being placed on the introduction of elements of true Artificial Swarm Intelligence that would serve as the primary control system of the drones with a secondary human control element as a fail-safe.

Thus, the primary control system would be used for Intelligence, Surveillance, Reconnaissance (ISR) tasks due to the wide swaths of water or land to be monitored, whilst the human element would be involved in the approval of using weapon systems against possible attackers.

At the same time, an increased level of attention should be granted to the issues of encrypted underwater communications and machine learning. This last issue could be addressed through the development of bio-inspired solutions (Hunt 2019).

Conclusion

Both of the cases mentioned above show clear levels of structural weaknesses in both the military and civilian infrastructure of a number of countries, such the US or a number of its allies, these weaknesses representing the creation of modern-day chokepoints that can have a considerable impact on a country's national security and war-fighting capabilities.

While the first type of operation (space) can achieve its' objectives in an efficient manner only through the usage of state-supported, joint forces, the second one (information) could be accomplished by using maritime assets, possibly international forces.

Even though both of these scenarios could be executed in a stand-alone manner, the effects of the combined usage of the actions mentioned above could outweigh the massive costs of such an undertaking, the main international actors that could direct and execute this kind of operation. Also, the evidence shows that mainly the Russian Federation and the People's Republic of China are initiating steps in order to reduce their vulnerabilities to the above-mentioned types of attacks, whilst enhancing their (possibly joint) arsenal in order to enact this types of actions.

Bibliography

Agency, The European Space. 2008. *Titan's surface organics surpass oil reserves on Earth.* 02 13. Accessed 03 21, 2022. https://www.esa.int/Science_Exploration/ Space_Science/ Cassini-Huygens/Titan_s_surface_organics_surpass_oil_reserves_on_Earth

Bodner, Matthew. 2018. *As Trump pushes for separate space force, Russia moves fast the other way.* 07 21. Accessed 21.03.2022. https://www.defensenews.com/ global/europe/2018/06/21/as-trump-pushes-for-separate-space-force-russia-moves-fast-the-other-way

Chuter, Andrew. 2020. *Former fighter picked to lead British military's space command.* 01 15. Accessed 21.03.20221. https://www.defensenews.com/global/europe/2020/01/15/ former-fighter-pilot-picked-to-lead-british-militarys-space-command/

David, Leonard. 2019. *Trump Officialy Establishes US Space Force with 2020 Defense Bill Signing.* 12 21. Accessed 21.03.2022. https://www.space.com/trump-creates-space-force-2020-defense-bill.html

Doocy, David. 2011. "Section 3: Operations, Chapter 14: Launch." In *Basics of Space flight*, by David Doocy, 207-223. Pasadena: Bluroof Press.

Erwin, Sandra. 2019. *Five things to know about U.S. Space Command.* 10 23. Accessed 03 09, 2022. https://spacenews.com/five-things-to-know-about-u-s-space-command/

Gray, Alexander. 2016. *This map shows how undersea cables move internet traffic around the world.* 11 24. Accessed 21.03.2022. https://www.weforum.org/agenda/2016/11/this-map-shows-how-undersea-cables-move-internet-traffic-around-the-world/

Greshko, Michael. 2018. *See all the world's active launch sites.* 10 04. Accessed 21.03.2022. https://www.nationalgeographic.com/science/2018/10/news-spaceports-cosmodromes-maps-world-space-week/

Hsu, Jeremy. 2008. *Vanguard 1, First Solar-Powered Satellite, Still Flying at 50.* 03 18. Accessed 21.03.2022. https://www.space.com/5137-solar-powered-satellite-flying-50.html

Hunt, Edmund. 2019. *The social animals that are inspiring new behaviours for robot swarms.* 03 27. Accessed 21.03.2021. https://theconversation.com/the-social-animals-that-are-inspiring-new-behaviours-for-robot-swarms-113584

Iriarte, Mariana. 2016. *MUM-T Operations on the U.S. Army's UAS roadmap.* 04 19. Accessed 22.06.2022. https://militaryembedded.com/unmanned/isr/mum-t-armys-uas-roadmap

Ji, Elliot, Michael B. Cerny, and Raphael J. Piliero. 2020. *What Does China Think About NASA's Artemis Accords?* 09 17. Accessed 21.03.2022. https://thediplomat.com/2020/09/what-does-china-think-about-nasas-artemis-accords/

Kharpaol, Arjun. 2019. *The 'splinternet': How China and the US could divide the internet for the rest of the world.* 02 03. Accessed 21.03.2022. https://www.cnbc.com/2019/02/04/the-splinternet-an-internet-half-owned-by-china-and-the-us.html

NASA. 2019. *What is GPS?* 06 03. Accessed 09.02.2021. https://www.nasa.gov/directorates/heo/scan/communications/policy/what_is_gps

NavalDrones. n.d. *Klavesin-1R ("Harpsichord").* Accessed 21.03.2022. http://www.navaldrones.com/Klavesin-1R.html

NAVALTODAY.COM. 2018. *Russia releases first video footage of new Kanyon/Status-6 nuclear torpedo.* 07 19. Accessed 21.03.2022. https://navaltoday.com/2018/07/19/russia-releases-first-video-footage-of-new-kanyon-status-6-nuclear-torpedo/.

Ni, Adam, and Bates Gill. 2019. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief, Volume 19, Issue 10,* 05 29.

Palkowsky, Deganit. 2021. *Why Russia Tested Its Anti-Satellite Weapon.* 12 26. Accessed 21.03.2022. https://foreignpolicy.com/2021/12/26/putin-russia-tested-space-asat-satellite-weapon/

Peter, Laurence. 2018. *What makes Russia's new spy Yantar special?* 01 03. Accessed 21.03.2022. https://www.bbc.com/news/world-europe-42543712

Ruiz Leotaud, Valentina. 2021. *Scientists explore possibility of mining iron, nickel, cobalt-rich near-earth asteroids.* 10 11. Accessed 21.03.2022. https://www.mining.com/scientists-explore-possibility-of-mining-iron-nickel-cobalt-rich-near-earth-asteroids/

TeleGeography. n.d. *Submarine Cable Map.* Accessed 21.03.2022. https://www.submarinecablemap.com/

United States, Executive Office of the President [Donald J. Trump]. 2020. *Executive Order on Encouraging International Support fot the Recovery Support for the Recovery and Use of Space Resources.* 04 06. Accessed 21.03.2022. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-encouraging-international-support-recovery-use-space-resources/

Wakefield, Jane. 2019. *Russia 'successfully tests' its unplugged internet.* 12 24. Accessed 21.03.2022. https://www.bbc.com/news/technology-50902496

Weitering, Hanneke. 2019. *France Is Launching a 'Space Force' with Weaponized Satellites.* 08 02. Accessed 21.03.2022. https://www.space.com/france-military-space-force.html.

SECTION IV

Technologies, Military Applications, Simulations And Cyberspace