Chatham House report: Space – NATO cyber security's weak spot

Authors:

Liina Lumiste (née Hirv)

In 2018, Norwegian military and allied officials confirmed that Russia had disrupted NATO's Trident Juncture exercise in Europe's High North region by persistently jamming GPS signals during the exercise. China has claimed 'the ability to use space-based systems and to deny them to adversaries as central to modern warfare'. As the dependence of military operations on space-based assets has increased exponentially over the last few decades and space-based assets are potential targets for cyber attack, the newly released Chatham House research paper 'Cybersecurity of NATO's Space-based Strategic Assets' suggests that NATO should bring space more to the spotlight. The research paper lists cyber threats to space-based strategic assets and capabilities, analyses capability requirements and gives concrete recommendations for ways improve the resilience of the space-based systems.

Space-based assets as targets for cyber attacks

Strategic military systems depend on space-based assets for the provision of data and for many capabilities, such as positioning, navigation and timing (PNT), intelligence, surveillance and reconnaissance (ISR), missile defence, communications, space situational awareness (SSA) as well as environmental monitoring. For accurate timing and navigation in PNT systems, NATO uses the global positioning system (GPS) which is also well known and widespread in civil use. ISR information and imagery is collected through surveillance and reconnaissance sensors. Both systems are satellite-based. Unmanned aerial vehicle (UAV) systems also rely on satellite-based 'beyond-line-of-sight' communication. These are only a few of the possible examples. In addition to the abundance of capabilities, it is noteworthy that the capabilities are also linked and therefore affecting one capability may cause collateral effects on others.

As explained in the Space Threat Assessment 2018 published by the Centre for Strategic and International Studies (CSIS), there are several intrusion points for space-based assets: antennas on satellites and ground stations, landlines that connect ground stations to terrestrial networks, and user

corrupted data in the system, or even the permanent loss of a satellite. As with every other technology, people have the potential to be the weakest link in the cyber defence of space-based assets – social engineering is an important tool for the adversary.

Vulnerabilities

The research paper highlights some of the most important vulnerabilities: use of commercial companies; 'back-doors'; dual use of satellites; and supply chain security of space technology. Chatham House reports have touched on these topics before. The question of supply chain was raised in the Livingstone and Lewis 2016 report, which observed that there was no coherent global organisation with regard to cyber security in space and that existing approaches had only limited reach into the supply chain. In this year's research paper, it is again stressed that when the supply chain does not ensure that military security standards are met, items procured may expose NATO systems to vulnerabilities.

NATO by itself does not own satellites, but is dependent on member states. In case of need, NATO requests access to products and services from the allies. NATO allies procure equipment and software, which will be integrated into their national defence infrastructure. In most cases, military and commercial assets are not separate. Therefore, NATO does not rely only on military assets, but also uses commercial, civilian and national or multinational assets for operations. Even though commercial methods have proven to be effective, they are accompanied by the inherent risk of lower security requirements. Data exchange between civil and military sectors may cause extra vulnerabilities. As most of the space-based capabilities are dual-use, meaning that assets are used both for military and civilian purposes, the Chatham House research paper recommends that operators 'apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications'.

The research paper also highlights the aspect of NATO's dependency on member states for communication capacity as a possible source of vulnerabilities. NATO owns satellite communications (SATCOM) ground stations, but no satellites; it is therefore highly reliant on allies to provide space-sourced data, information and services. In addition, ensuring the security of space capabilities is mostly in the hands of the allies. This puts NATO into a position where its main option to protect capabilities of vital importance is to encourage allies to put effort into securing the space-based assets and foster cooperation in space-based systems cyber security.

Space as a domain of operations?

During the Brussels Summit in 2018, the Alliance recognised space as a 'highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture' and on 27 June 2019, it approved new space policy. As claimed by NATO's Secretary General, Jens Stoltenberg, the

about information sharing and increasing interoperability. The research paper suggests that, in addition to policy, NATO needs to agree upon space doctrine. While policy directs, assigns tasks and prescribes desired capabilities, doctrine provides principles of how operations should be planned, prepared, commanded, conducted, sustained, terminated and assessed.[1]

This suggestion becomes even more relevant when taking into consideration recent announcements by some NATO diplomats about NATO's aims to recognise space as a domain of warfare during the London summit at the end of 2019. This indeed would be a big step towards focusing more on space-based assets and their vulnerabilities. Considering the current context, in which China and Russia are increasing their presence in space, this action by NATO is inevitable. Whether or not NATO claims space as a domain, adversaries will nevertheless develop their aggressive capabilities, from cyber operations to anti-satellite missiles. Therefore, it is prudent to update the approach towards space and space-based assets to face new challenges.

Yet, claiming space to be a domain of warfare highlights legal considerations. The Chatham House research paper raises a question from the cyber perspective: whether a cyber attack on a space system has to have kinetic consequences in order to give grounds for collective self-defence according to the Washington Treaty. This can be supplemented with a question on whether causing kinetic consequences that result in debris breaches the responsibility not to cause widespread, long-term and severe damage to the natural environment, as stipulated in article 35 of Additional Protocol I to the Geneva Conventions of 12 August 1949.[2]

Another question raised is targeting dual-use space technology in international humanitarian law (IHL). The principle of distinction foresees the duty to distinguish between the civilian population and combatants and between civil and military objects. As in the case of cyber objectives,[3] dual-use satellites should be counted as military objectives, but would be subject to the rule of proportionality and requirement to take precautions in attack.[4]

Conclusion

The Chatham House research paper makes recommendations that more or less all stress the same things: NATO is highly dependent on space capabilities; space-based systems are vulnerable to cyber attacks and will become more and more appetising targets for adversaries; and NATO must foster cooperation and information sharing between member states. Overlooking these aspects could undermine the credibility of the information provided through the space-based systems, which would in turn affect deterrence and strategic liability. In the broader view, destabilising space-based assets would not only affect military conduct, but also have severe effects on civil infrastructures.

1. (AJP)-01 Edition E, Version 1, Allied Joint Doctrine, 2017, NATO Standardisation Office. [↩]
2. See longer discussion on this matter in M. Bourbonnière „Law of armed conflict (LOAC) and the neutralisation of satellites or ius in bello satellitis‘, Journal of Conflict and Security Law, Volume 9, Issue 1. [↩]
3. See Rule 101 in Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017. [↩]
4. M. Bourbonnière, note 2. [↩]

← Library

The NATO Cooperative Cyber Defence Centre of Excellence

ccdcoe-at-ccdcoe.org
+372 7176 800
Address: Filtri tee 12, Tallinn 10132, Estonia

Twitter
Youtube
Flickr
Facebook