I. The space–cyber nexus

NIVEDITA RAJU AND LORA SAALMAN

There is a distinct overlap between the domains of space and cyberspace. For example, space assets rely on cyber components for the transmission and storage of data, making them vulnerable to cyberattack or harmful interference.[1] Equally, cyber assets rely on satellite and communications networks that are vulnerable to physical attacks.[2]

The term 'counterspace' is broadly used to refer to capabilities or techniques used to disrupt or damage another entity's space object (belonging to either a state or non-state actor), with the objective of gaining superiority over an adversary. It can refer to both kinetic and non-kinetic attacks against space systems. Kinetic attacks rely on physical destruction of the target using, for example, direct-ascent or co-orbital anti-satellite (ASAT) weapons. Non-kinetic attacks may or may not cause physical damage to the system; for example using lasers to blind the optical sensors of a satellite, cyberattacks against satellites, or electronic attacks targeting the electromagnetic spectrum (e.g. jamming satellite signals).[3]

A cyberattack is an action designed to target a computer or any element of a computerized information system—such as the digital components of a space system—to change, destroy or steal data, as well as to exploit or harm a network.[4] Cyberattacks are related to, but distinct from, a cyber intrusion, which causes digital systems to enter an insecure state.[5] An intrusion often serves as the preliminary preparation and penetration required to carry out a cyberattack. Among the malware used to carry out the cyberattacks featured in this chapter are backdoors, ransomware, trojans and wipers (see box 11.1 and the examples in sections II–IV).

There are two further aspects of the overlap between the space and cyberspace domains: the difficulty of applying international law and the challenges with respect to international governance.

[1] Weeden, B. and Sampson, V. (eds), *Global Counterspace Capabilities: An Open Source Assessment* (Secure World Foundation: Broomfield, CO, Apr. 2022).

[2] See e.g. United Nations, General Assembly, Open-ended working group (OEWG) on reducing space threats, 2nd session, Statement by Russia, 12 Sep. 2022, p. 2.

[3] On electronic warfare see also Raju, N., 'A proposal for a ban on destructive anti-satellite testing: A role for the EU?', EU Non-Proliferation and Disarmament Papers no. 74, EU Non-proliferation and Disarmament Consortium, Apr. 2021, p. 2.

[4] Computer Security Research Center, 'Cyber attack', US National Institute of Standards and Technology, Information Technology Laboratory.

[5] National Initiative for Cybersecurity Careers and Studies, 'Cyber intrusions', US Cybersecurity and Infrastructure Security Agency, 17 Sep. 2018.

Box 11.1. Some types of malware used in cyberattacks

Backdoor

A backdoor allows access to a computer system or encrypted data through bypassing the system's security mechanisms.

Ransomware

Ransomware threatens to publish the victim's data or permanently block access to it unless a ransom is paid.

Trojan

A trojan downloads malware disguised as a legitimate programme onto a computer.

Wiper

A wiper erases user data and partition information from attached drives, making the system inoperable and unrecoverable.

Source: Baker, K., 'The 12 most common types of malware', Crowdstrike, 28 Feb. 2023.

Among the challenges when it comes to international governance is attribution of offensive cyber activities under international law.[6] It can be difficult to identify and verify the source of an attack, potentially allowing states to avoid accountability. The Viasat cyberattack in February 2022 (see section II) illustrates further hurdles to regulation in that most space systems serve both civilian and military functions (i.e. they are dual-use) and they frequently have users in multiple states that may not be involved in a conflict. These factors raise questions as to when and how these systems can be lawfully targeted during armed conflict in a way that conforms to the strict requirements of international humanitarian law.

Under international humanitarian law, civilian objects—such as satellites providing civilians with essential services—cannot be targeted.[7] If the space system is dual-use—for example, it provides communications services to both the armed forces of the state and civilians—then it may only be lawfully targeted if it qualifies as a military objective by its nature, location, purpose or use.[8] Furthermore, indiscriminate attacks—including attacks which may cause 'incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'— are prohibited.[9] Legality is even more complex when a state targets space systems that also have an impact on third-party states that are not involved in the conflict. In certain

[6] Kastelic, A., *Non-escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics* (UNIDIR: Geneva, Jan. 2022).

[7] Protocol Additional to the 1949 Geneva Conventions, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I, AP I), Article 48. For a summary and other details of the protocol see annex A, section I, in this volume.

[8] Additional Protocol I (note 7), Article 52.

[9] Additional Protocol I (note 7), Article 51.

situations, the rules governing neutrality may apply. For example, in a potential armed conflict between two states, a third state that seeks to be neutral must practice 'impartiality' by treating both belligerent states equally.[10] This can be complicated in the space domain because satellites are owned and operated not only by states but also by private entities, indicating scenarios in which the 'neutral' status of a state may be called into question.[11]

Since 2004 the United Nations has worked through its groups of governmental experts (GGEs) and open-ended working groups (OEWGs) to develop principles for responsible state behaviour in cyberspace and on information and communications technology (ICT) in the context of international security (see section IV). Their work is reflected in regular reports through which UN member states have developed and adopted a set of voluntary norms that describe what states should and should not be doing in cyberspace. Some of the norms are actions that states want to encourage, while others involve actions that states should avoid, such as knowingly allowing their territory to be used to conduct cyberattacks or attacks targeting civilian critical infrastructure.

The UN has also established GGEs and, more recently, an OEWG on space security governance. Threats arising at the space–cyber nexus were the subject of discussion at the September 2022 meeting of the OEWG, which focuses on developing norms, rules and principles of responsible behaviour to reduce threats to space systems (see section III). Many exchanges at this OEWG referred to the parallel forums for cyber governance, which some suggested could inform future approaches to the governance of cyberattacks on space systems, while others expressed concern regarding overlaps in the subject matter being discussed in parallel processes.[12] There are differences in the governance of both domains—notably that, unlike cyber, the space domain has been governed by legally binding treaties for decades. However, the attacks in Ukraine (see section II) highlight the need to ensure that ongoing multilateral processes on space and cyberspace governance are consistent and informed by each other's work. This can in turn ensure that any norms, rules or principles proposed in these processes are reinforced. Indeed, in the OEWG session the German delegation pointed to their national submission

[10] Koplow, D. A., 'Reverse distinction: A US violation of the law of armed conflict in space', *Harvard National Security Journal*, vol. 13 (2022), pp. 100–102.

[11] Koplow (note 10), p. 102.

[12] For comments on the scope for consistency between space and cyber processes see e.g. the German delegation's comments in the general exchange between member states at the 10th meeting, 2nd session of the UN OEWG on reducing space threats, 16 Sep. 2022, UN Web TV, 01:04:47–1:07:00. For concerns about overlap see e.g. the Russian delegation's comments in the same forum at 00:26:08–28:08.

to the UN secretary-general in 2021 regarding responsible behaviours in outer space, which was informed by work in the cyber process.[13]

Diverse activities have also been carried out by the private sector in coordination with governments in both space and cyberspace. For example, the US government requested that Microsoft share with European states details of the malware FoxBlade that Microsoft discovered in Ukraine.[14] In addition, Mykhailo Fedorov, a Ukrainian vice-prime minister, requested SpaceX to provide Ukraine with access to its Starlink satellite internet service and asked cryptocurrency exchanges and even the Internet Corporation for Assigned Names and Numbers (ICANN) to implement sanctions against Russia.[15] Such cooperation between government and industry provides scope for exploring how to effectively advance governance for both space and cyberspace in a manner that accounts for the nexus between the two domains. However, some of this cooperation, particularly in relation to offensive cyber operations, is likely to add to the regulatory complexity. These issues are explored in the following sections.

[13] See the German delegation's comments (note 12); and United Nations, General Assembly, 'German national contribution to the secretary general in reference to the Resolution 75/36 on norms, rules and principles of responsible behaviours in outer space', Submission by Germany, Apr. 2021.

[14] Sanger, D. E, Barnes, J. E. and Conger, K., 'As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war', *New York Times*, 28 Feb. 2022.

[15] Brodkin, J., 'Ukraine asks Musk for Starlink terminals as Russian invasion disrupts broadband', Ars Technica, 28 Feb. 2022; and Fedorov, M., Letter to the Internet Corporation for Assigned Names and Numbers (ICANN), 28 Feb. 2022.