11. Space and cyberspace

Overview

The space and cyberspace domains featured prominently in the war in Ukraine in 2022, illustrating their overlap: the space–cyber nexus. There are three aspects to this overlap (see section I). First, there is scope for cyberattacks to be directed against space systems, in particular the digital components on which they rely to transmit data. Second, the two domains share similar challenges with respect to international governance due to the difficulties in attributing the source of attacks and in establishing state accountability. Third, international law, including international humanitarian law, applies to both the space and cyberspace domains, yet because their systems are often dual-use—serving both civilian and military functions—and used by multiple states, there are questions regarding lawful targeting of such systems.

The war in Ukraine demonstrated the growing significance and confluence of these two domains, where space systems and a range of other critical infrastructure were the target of persistent cyberattacks (see section II). These included a cyberattack on the ground terminals of a commercial satellite communications company, which had ripple effects across Europe. Cyberattacks were also directed against key Ukrainian governmental departments, such as its defence ministry and armed forces. Cyberattacks further targeted organizations in the information technology, agricultural and financial sectors, and disrupted Ukrainian telecommunications networks and power facilities.

These attacks at the nexus of the space and cyber domains disrupt or deny essential services, either temporarily or permanently. Because the attacks are difficult to attribute, discussions in multilateral forums about the governance of space and of cyberspace have highlighted the need for further measures to clarify state accountability and prevent or mitigate impacts on civilians.

In terms of space governance, a small but significant step towards new measures was the successful adoption of a resolution banning destructive, debris-generating, direct-ascent anti-satellite (DA-ASAT) missile tests by a majority of states at the United Nations General Assembly (see section III). Destructive DA-ASAT tests were among the threats to space systems discussed at the UN open-ended working group (OEWG) on reducing space threats, which convened under Resolution 76/231 for its first and second sessions in 2022.

In terms of cyber governance, the OEWG on 'security of and in the use of information and communications technology 2021–2025' continued its work in the face of the challenging geopolitical environment (see section IV). The First Committee of the General Assembly welcomed a proposal for a programme of

action (POA) to continue as a permanent, inclusive, action-oriented mechanism after the conclusion of the current OEWG. Nevertheless, this proposal remains contentious, as does participation in these UN meetings by the private sector and non-governmental organizations. Further, the ongoing cyberattacks on civilian critical infrastructure—allegedly conducted by both Russian and Ukrainian state and non-state actors before and during the Ukraine conflict—demonstrate the difficulty in enforcing the voluntary norms formulated during the ongoing UN process.

The activities and mechanisms required to enforce cyberspace norms are far from dormant, however. Cyber capacity-building and confidence-building measures have been developed under the second OEWG, including the development of a points of contact directory. In addition, international policing collaboration in apprehending cybercriminals has been evolving, not only with Ukraine but even between Russia and the United States. The 2022 international summit of the Counter Ransomware Initiative provided an action plan against ransomware, which is being leveraged for cyberwarfare as well as cybercrime aims. Cooperation with industry has also been expanding, as with a request by the US government for Microsoft to provide the code of FoxBlade malware to European countries to help them combat cyberattacks.

Government collaboration with the private sector in cyberspace mirrors the space domain, where commercial actors are increasingly engaged to support military services. In particular, Russian statements regarding the potential targeting of commercial space assets that support Ukrainian military services imply potential escalation and impacts on governance. However, some states' objections to the involvement of non-governmental organizations and the private sector in UN processes governing space and cyberspace pose longer-term challenges for engaging both governmental and non-governmental stakeholders in the creation of norms and their enforcement.

NIVEDITA RAJU AND LORA SAALMAN