

Space Security Roundtable — May 18, 2018

Responding to Unconventional Threats to Europe's Space Operations CONCEPT PAPER

Space assets are essential for the proper functioning of European societies, economies, security and well-being. The disruption of the services they provide, would hamper, and likely cripple, several aspects of our day-to-day lives. Accordingly, space infrastructure requires enhanced resiliency to ensure critical functions performance and overall mission assurance. Its cross-border (physical and service-level) and cross-sector (e.g. transport, telecommunications, trade and banking, defense etc.) interdependencies expose it to a variety of risks and threats. These threats could result in the compromising of satellites, ground stations or links and trigger a cascading effect. Military systems represent the most obvious targets, but civil and commercial satellites provide many critical support functions for society, defense, security and political operations (e.g. communications and reconnaissance) that also make them vulnerable to attacks.

Naturally, a number of safeguards and processes have been adopted to mitigate various risks and threats to these systems. Traditionally, however, the security dimensions of civil and commercial space activities have focused largely on risks related to environmental and technical issues. While these remain important and valid undertakings, there is another set of capabilities being deployed by Europe's competitors and foes that span national security, civil and commercial space activities. As Europe now has operational space infrastructure, it is important to also consider new unconventional (or hybrid) risk factors that are considerably more prominent than in the past.

These space hybrid threats (i.e. intentional, mostly reversible, and often harmful, space actions/activities conducted just below the threshold of requiring a meaningful military or political retaliatory response) are closely linked to the strategic interests of major space competitors (notably China and Russia). These threats are almost sure to grow as space serves as a means to project power, control, and influence for the purpose of consolidating major space competitors' strategic objectives (both industrial and military).

Among the most vexing challenges presently confronting both the European public and private sectors is understanding, and responding to, the risks and threats to space that stem from the pursuit of these strategic goals.

Targeted "grey-zone" operations challenge the current space governance regime. The dual-use nature of space assets makes it often difficult to ascertain threatening behavior. Although certain mechanisms exist, there is a growing consensus that more needs to be done to organize European governments to map and track those activities that have the potential to undermine significantly the resiliency of deployed space systems, as well as configure sound preventative and crisis management policies.

Military and civilian decision-makers must have communications and other tools instantly available when faced with hostilities attributed to a state actor (something such actors seek to avoid). Labeling these threats as symptoms of hybrid warfare could help stimulate intensified and expanded dialogue within Europe as well as with partners in the U.S., Asia and elsewhere. The private sector also needs to be fully engaged with respect to real time communications, resilience and appropriate deterrence. Developing these capabilities should be undertaken in parallel with the evolution of international law for the space domain – namely institutionalizing norms of responsible behavior.

Today, space hybrid threats are often glossed over or only considered in classified settings. Greater public awareness and support could prove of real value to decision-makers. By establishing a foundational definition of these space hybrid operations, European nations can build a political case for targeted, proportional responses to this kind of low-intensity conflict environment on a pre-approved basis. By not responding, an atmosphere of permissiveness (and negative norms of behavior) is fostered and the potential for triggering an escalatory spiral is elevated.

Newly granted authorities and inter-ministerial/inter-agency lines of communications are urgently required to defend against the perils emanating from the frequent testing of sophisticated counterspace capabilities. Remedies include enhanced situational awareness and early warning, a rapid capability to discriminate between normal and hostile activity, and the ability to anticipate security-related knock-on effects (e.g. the short-term impact of losing certain space-related services etc.).

This closed roundtable is designed to take advantage of the expertise of the senior participants assembled in order to provide a better understanding of this issue and help facilitate a more informed policy framework concerning how we protect our space assets (including ground infrastructure) and the critical benefits and capabilities derived from them. The proceedings will be held under the Chatham House Rule to facilitate candid exchanges on these somewhat sensitive subjects.