Time to designate space systems as critical infrastructure

The bottom line? The Executive Branch must designate space systems as a critical infrastructure sector and Congress must provide the Sector Risk Management Agency (SRMA) with the resources needed to execute the mission.

Credit: SpaceNews/Midjourney illustration

Frank J. Cilluffo is director of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. He also served as a commissioner on the U.S. Cyberspace Solarium Commission. **RADM (Ret.) Mark Montgomery** is senior director of the Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies. He is also executive director of the

Cyberspace Solarium Commission (CSC) 2.0.

Space systems are fundamental to U.S. national and economic security — but we have not been organizing or resourcing ourselves in a way that is consistent with this reality. Despite the fact that an array of critical infrastructure and national critical functions rely on space systems, they are not one of our designated critical infrastructure sectors. As a result, space systems are not being treated as the priority that they need to be, particularly when we are in the midst of a 'space race' with China, as the administrator of NASA recently stated bluntly.

Consider what space systems are foundational to operating: telecommunications systems; positioning, navigation and timing (PNT) for nearly all automated ground-based systems; the global positioning system (GPS); military operations and mission assurance; intelligence, surveillance and reconnaissance; the financial services. energy and water sectors—and the list goes on. U.S. economic prosperity is likewise bound up with space systems. In 2021, $469 billion in global revenue was generated in space. As off-Earth and in-space activities such as mining and manufacturing come into being and expand, this number will grow and space systems will hold an ever-more important role.

Designating space systems—meaning the ecosystem from

ground to orbit, including sensors and signals, data and payloads, and critical technologies and supply chains—as a critical infrastructure sector would facilitate a more organized, focused, and coherent approach to risk management, launch authorization, and public-private collaboration. It would signal inside and outside the country that space security and resilience is a U.S. national security priority. And it would marshal the focus, resources and collaboration needed to mitigate the unique cybersecurity challenges that present in this context, including legacy technologies and the difficulty of repairing or replacing systems in orbit.

Getting the country to where it needs to be will require action from all concerned parties: Congress, the Executive Branch, and industry — plus industry and government together, as the commercial space community continues to innovate and evolve and occupy an increasingly important place in the space systems sector. Our recently released policy paper, undertaken as part of the Cyberspace Solarium Commission (CSC) 2.0 initiative, lays out an action plan with specific steps recommended for each key actor.

The bottom line? We will not achieve liftoff unless two things happen: the Executive Branch must designate space systems as a critical infrastructure sector and Congress must provide the Sector Risk Management Agency (SRMA)

with the resources needed to execute the mission.

Granted, even those who agree on the criticality of space systems disagree on how best to protect them. In our view, however, only NASA possesses the wide range of capabilities needed to act as lead SRMA — and even NASA requires additional resources to enhance its capabilities to meet the mission and do so at no expense to its existing work. This is where Congress comes in. An initial investment of at least $15 million per year into developing NASA's SRMA capabilities would make all the difference. With but a few exceptions, the federal government has generally not put its money where its mouth is when it comes to SRMAs. When it comes to space systems, the government needs to walk the talk.

We also need to make sure that our laws are serving us well in that they reflect and respond to current realities and needs. To this end, the Congressional Research Service (CRS) should be directed to undertake a review to determine what legislation is needed to account for the expansion of commercial space operations. On the other hand, the Executive Branch should not assign the SRMA a regulatory role. Space systems are already regulated through other rule sets — and our efforts would be best spent streamlining and simplifying compliance with existing regulations.

Government must also offer to industry a clear value

proposition for the way forward. And where good work is already underway, we should not disrupt it. This is why there should be two directed subgroups within the space systems sector — one run by the Department of Defense and Intelligence Community jointly concerning defense and intelligence systems, and another run by the Federal Communications Commission (FCC) for communications systems. Additionally, the newly created Space Council can work to ensure smooth cooperation between federal agencies as NASA takes on the role of SRMA.

Efforts to enhance the security and resilience of space systems will require close cooperation with both domestic and international partners. At home, we must create a risk management enterprise that effectively pairs commercial and government capabilities and affords the commercial space community an instrumental role in the governance of the space systems sector. In tandem, Washington must lead by example and work with allies and industry to develop and strengthen internationally accepted norms of responsible behavior in space.

The challenge is considerable, but we can leverage and build upon existing work such as that of Information Sharing and Analysis Centers, including the Space ISAC, and at the Space Council — which just days ago convened the Space Systems Cybersecurity Executive Forum jointly with the

Office of the National Cyber Director, consistent with the administration's new National Cybersecurity Strategy. Without accompanying and concerted leadership from Congress and NASA and other federal agencies, however, we will fall short of where we need to be — at a time when China is honing its ability to strike satellites using cyber operations, electronic warfare and other means; and Russia has hacked U.S. satellite communications networks. Clearly, time is not on our side. We should move quickly to designate space systems as a national critical infrastructure and treat them accordingly.

RADM (Ret.) Mark Montgomery is senior director of the Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies. He is also executive director of the Cyberspace Solarium Commission (CSC) 2.0
More by Mark Montgomery