REMARKS - Emerging Threats: Outer Space, Cyberspace, and Undersea Cables

- Arms Control Today

January/February 2017

By Frank Rose

In 2015, approximately 97 percent of the world's transoceanic communications transited over privately held, commercial, undersea fiber-optic communications cables. A large-scale outage of these undersea cables would affect critical governmental and business operations, communications, financial transactions, logistics, and transportation. We are concerned that potential adversaries may be looking for vulnerabilities in undersea cables around the world.

Cyberthreats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyberthreat actors, methods of attack, targeted systems, and victims are also expanding. Adding to the problem, it is not always easy to identify the origin of such attacks.

Further, our reliance on international space systems has risen to an unprecedented global scale. We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems. In addition, threats to space systems from debris or irresponsible activities are increasing. In particular, we are concerned by Chinese and Russian pursuit of weapons systems to destroy satellites in orbit. The debris created from such activities lingers uncontrollably, thus creating the potential for impacts far beyond the destruction of an individual targeted satellite.

We should not look at space, cyber, and undersea cables independently of one another. If a determined adversary wants to cut off U.S. and allied access to communications infrastructure, it is likely to deploy capabilities to attack space, cyberspace, and undersea cables at the same time, in a coordinated manner, and across a broad spectrum of means.

There are also cross-domain vulnerabilities. What happens in outer space won't stay in outer space. Satellites are vulnerable to cyberintrusions, as we saw take place in 2014 when a cyberattack compromised four U.S. weather satellites. Banking, mapping, and other essential parts of the global internet infrastructure are dependent on space assets for services such as timing and location data. Additionally, space and cyberassets are vital to our deterrent and defensive capabilities, including communications, positioning, and nuclear command and control. It is easy to see how attacks in these domains could lead to a wider kinetic conflict.

It is interesting to see where there are linkages in the policy and diplomatic approach to addressing these threats, especially in space and cyber domains. A common thread is the lack of widely accepted and enforceable norms of responsible behavior. There are existing treaties on space policy and undersea cables, whereas none currently exist relating to cyberspace. In space and cyberspace, we face similar challenges to pursuing traditional arms control, given the dual-use nature of these systems, the number of actors, and the challenges of attribution and verification. To address these challenges, we have worked to pursue consensus among states that international law applies in both domains and further clarify how foundational laws, such as the law of armed conflict and the UN Charter, apply.

So what does any of this have to do with nuclear arms control and disarmament? Continued progress in reducing nuclear arsenals cannot be divorced from the global security environment or our unconditional commitment to the security of our allies. Ensuring security depends in part on our success in constructing mutually agreed-on norms that referee behavior in these largely unregulated domains. Establishing clear rules of the road in these realms can help create the security conditions for future nuclear arms reductions.

Going forward, we must enhance and communicate our cross-domain deterrence in a credible manner to achieve and maintain stability. This effort will require better monitoring and verification capabilities to make attribution easier. We also need to be working more closely with our allies. Our worldwide system of alliances is a true "asymmetric advantage" of the United States. Meanwhile, we must look within our own government to ensure we are taking a whole-of-government approach and to avoid the instinct of stove-piping that can paralyze the bureaucracy. I see this area as a priority for the U.S. government now and in the future.

Frank Rose is assistant U.S. secretary of state for arms control, verification, and compliance in the Obama administration. This piece is adapted from a December 2 speech at the University of Virginia.

Source URL: https://www.armscontrol.org/act/2017-01/news/remarks-emerging-threats-outer-space-cyberspace-undersea-cables