ISRAELDEFENSE

Day Thursday, ו' שבט התשע"ז
02.02.2017

Cybersecurity and Outer Space: Connected Challenges

Outer space and cyberspace are relatively new areas of human endeavor. Until recently, the connection between them did not draw the interest of international lawyers and outer space policymakers - but a change is now underway

Adv. Deborah Housen-Couriel | 2/02/2017

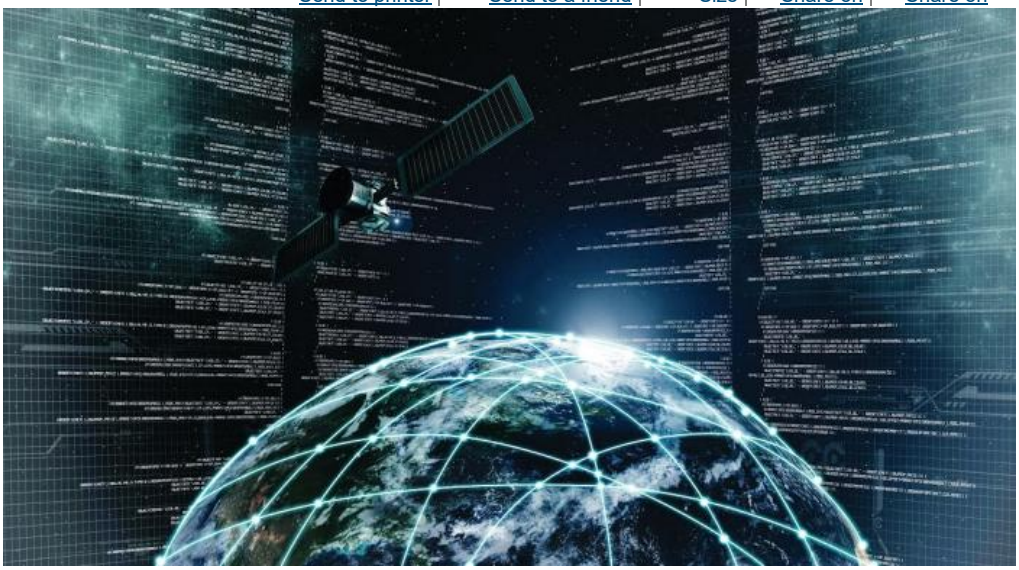


Illustration: Bigstock

The law of outer space and the law of cyberspace are both areas with which international law and international lawyers have been engaged for decades. The two areas of law are now beginning to draw the attention of experts for the ways in which they intersect and overlap, creating significant and interesting challenges for lawmakers and policy experts.

Suppose that a group of hackers intent on hijacking certain sensitive data monitor internet traffic that they know is relevant to their purposes and is also transmitted via geosynchronous satellite – a type of internet connection that is increasingly utilized for its accessibility to remote areas (despite latency issues) and that covers a wider geographical footprint than standard, land-based internet providers. The satellite's footprint can in fact extend over several countries, making efforts to track the physical location of a computer using a satellite IP address much more difficult than the tracking of a typical IP control server.

The hackers take advantage of precisely this vulnerability. They select a random IP address of Jane, an unsuspecting online user of such a satellite-enabled internet connection, and infect her now-targeted computer with malware that permits them to utilize her satellite IP address in order to hijack data from other similarly-infected machines. The technique they use, leveraging the broad satellite footprint, makes identification of their command server extremely difficult. And without it, the hack is nearly impossible to trace.

This abuse of satellite internet connections is exactly how the sophisticated Turla satellite hackers group operated for more than eight years, hijacking data with impunity from hundreds of computers in more than forty countries, including China, Russia and the US. Their modus operandi was exposed and fully detailed by Kaspersky analysts in 2015. In the words of one senior analyst, Stefan Tanase, "It's probably one of the most effective methods of ensuring their operational security…nobody will ever find

out the physical location of their command and control server. It can be anywhere in the range of the satellite beam."

The Turla hack, as well as other exploitation by hackers of satellite communications such as the exposure in 2016 of serious data breaches into US weather satellites that provide critical environmental data for weather forecasting; Iran's jamming of Eutelsat transmissions beginning in 2009; and the ongoing interference with NASA systems, highlights the fact that the outer space and the cyberspace domains are inextricably linked operationally. Communications with outer space via satellites occurs exclusively through the use of the electromagnetic spectrum, a fundamental building block of cyberspace. And as the dependence of critical computerized systems – whether space-based or land-based – on satellite communications grows, so does their common vulnerability to threat vectors in cyberspace.

Addressing the Legal Challenges

This operational intersection is also reflected in the relationship between the legal regimes that govern outer space and cyberspace. International legal norms that are applicable to each of these realms of human activity, as well as those to the other realms of land, sea and air, define what states, international organizations, companies and even individuals can and cannot do within the limits of the law. As with all human activities, strict conformity to these agreed norms is not always an assumption that can be made about the behavior of state and non-state actors.

Both outer space and cyber space have their share of "wild west" scenarios in which agreed norms are completely ignored.

Yet there are still significant state and organizational interests, initiatives and behaviors that carefully uphold the relevant agreed treaties, agreements, and general international law, as in the overall prohibition of the use of force codified in the UN Charter on the basis of earlier understandings among states, and the five treaties relating to outer space activities concluded in the 1960's and 1970's. One of these treaties, the 1971 Convention on International Liability for Damage Caused by Space Objects, establishes the norms for division of legal responsibility between states when satellites, space debris and other space objects cause damage to the property of another state, even at the launching stage. Such "damage to property" has been interpreted up until now as purely physical damage to satellites, yet virtual damage, such as the disruption or hijacking of satellite-relayed data, may also be considered under this provision in the future.

The intersection of space and cyber legal norms is also seen in the 1966 Outer Space Treaty (OST), which extends the norms of international law into outer space by agreement among its 105 signatories. Article 9 of the OST prohibits "harmful interference" with other states' activities in outer space, a term which includes undue interference with the use of the electromagnetic frequency spectrum resource utilized for satellite communications.

Several international fora and organizations have taken up the common challenge of merging the legal norms that apply in cyberspace and in outer space. NATO, the UN Office for Outer Space Affairs (UNOOSA), the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), and the Shanghai Cooperation Organization have all addressed issues that have legal and practical ramifications for both of these realms, especially around the prohibition of the use of force by states and their concomitant right to self-defense under the UN collective security regime. A recent UNOOSA conference in September 2016 recommended that the connection between cyber security and the security of space systems be further considered by the international community. Additionally, the MILAMOS project is currently examining the applicability of some aspects of international law to outer space, including cyber-related aspects.

These trends will continue to be critical in the coming years, as both outer space and cyberspace gain ever-increasing strategic importance for countries, international organizations, and private corporations. Norm-building efforts in both of these areas will also reveal the strategic concerns of decision-makers and lawmakers in governing these two relatively new realms of human endeavor.

***

Deborah Housen-Couriel's Tel Aviv law practice is supported by ongoing cybersecurity research at TAU-ICRC and the MILAMOS project

READ NEXT

Report: CIA was involved in the assassination of Mughniyah along with the

Hamas prepares for a future confrontation: Restores its tunnels and rocket sto...

Elbit Systems' ATMOS Arrived to Thailand

First F-35I 'Adir' Flight in Israel

Add new comment

PM Netanyahu to Address the Opening Plenary of CyberTech 2017

Final Preparation for CyberTech 2017

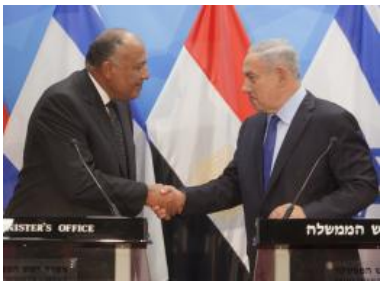
Operation "Golden Spear" in Yemen

Diplomacy and Israel's Nuclear Posture

You might be interested also

The Frail Israeli-Egyptian Defense Relations

Ehud Eilam | 29/01/2017



Israeli PM Netanyahu with Egyptian foreign minister Sameh Shoukry (Photo: AP)