

Telos Ghost: Protecting the Next Generation of Cybersecurity Professionals at Georgetown University

With the global demand for cybersecurity skills exceeding the number of qualified candidates, higher education institutions are adding cybersecurity career development programs to their curriculum to help fill the cybersecurity gap. Georgetown University's Master of Professional Studies in Cybersecurity Risk Management is designed to help cultivate the next generation of cybersecurity professionals. Its program integrates classroom learning with hands-on experience to prepare students to effectively protect organizations from today's ever-evolving cybersecurity threats and vulnerabilities.

A core component of the curriculum is the Cyber Intelligence Lab, which enables students to simulate real-life cyber threats and defense analyses to manage cyber surveillance operations. This work can unintentionally reveal the student's presence on the internet, the geographic location of the university, and even their identities as well as inadvertently open up attack surfaces for bad actors to exploit.

To ensure that the students work securely and privately, Telos Ghost®, a cloud-based obfuscation and non-attribution network, is used in the Cyber Intelligence Lab. Telos Ghost lets students securely log onto the internet and instantly blend into the background as nondescript web traffic. It hides their online activities, masks their identities, and misattributes their locations to hide their presence on the internet.

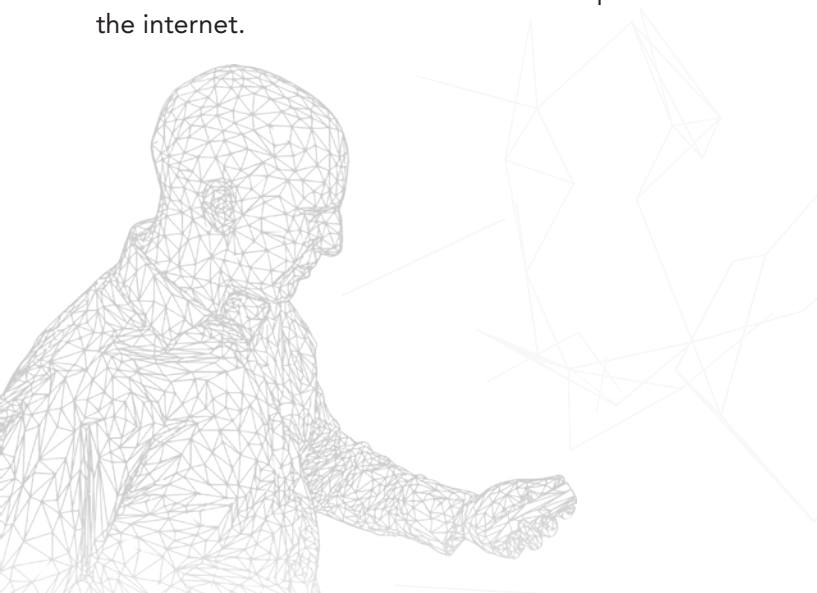
Telos Ghost's advanced capabilities include:

- **Dynamic IP routing:** Hides your online activities in a labyrinth of network nodes. A mesh of secure routers makes it impossible to determine the source or direction of network traffic.
- **Multi-layered encryption:** Makes your research data impenetrable. Multiple layers of encryption are applied to your data as it traverses the network to ensure that it is kept hidden from malicious actors looking for vulnerabilities in order to access your network.
- **Managed attribution:** Disguises your identity to ensure anonymity for your research activities.

With Telos Ghost's managed attribution, dynamic IP routing, and multi-layer encryption features, students can blend into their digital environment to avoid detection and work without fear of discovery. As an additional benefit, Telos Ghost eliminates cyberattack surfaces of internet-connected devices and networks, helping to prevent cyberattacks.

The network that Telos has established for Georgetown University is a completely virtual network that is entirely hosted in AWS. Being hosted in Amazon Web Services combines the inherent security of the AWS Cloud with the added layers of obfuscation to ensure ultimate protection from cyber adversaries.

Telos Ghost protects student identities, their work and Georgetown University by preventing them from being seen in the first place. To learn about Telos Ghost, visit www.telos.com/ghost.



Solutions that **empower** and **protect** the enterprise.™