DEFENDING the Internet

A four-course program at the NATO School prepares graduates to identify and foil cyber attacks

By Maj. Rob Meanley, director of academic operations, NATO School

Since its founding in 1953, the NATO School Oberammergau (NSO) in Germany has graduated more than 210,000 officers, noncommissioned officers and civilians from 88 nations. Recognized as the global leader in multinational education, NSO conducts operational-level training in support of NATO's strategy to enhance operational capability.

In this capacity, NSO promotes the framework for NATO organization, plans, policies, operations, procedures and instruction in the employment of, and defense against, selected weapons systems. In partnership with U.S. European Command and NATO, the NSO underpins all allied operations, strategy, plans and doctrine throughout the European theater and other partner nations.

Through NSO, NATO assures the Alliance's collective capability to neutralize security challenges, including cyber attacks, the proliferation of weapons of mass destruction, terrorism, energy vulnerabilities and other threats to the security of NATO's nearly 900 million citizens. As such, NSO's charter is to focus strategically on countering these ever-evolving challenges — not the least of which is the cyber warfare arena.

Cyber security certificate program

Considering that cyber threats are projected to increase exponentially during NATO's shift from an operational to contingency planning mindset, NSO has collaborated with the U.S. Naval Postgraduate School (NPS) in Monterey, California, to offer a cyber security curriculum. Beginning with a basic (intro-level) foundation, each course complements previous material, culminating with in-depth network traffic analysis and evaluations. Upon completing the rigorous, four-course program, graduates earn an NSO-NPS Cyber Security Program Certificate.

Although NSO recommends that students take all four courses in logical progression to ensure the highest comprehension and cyber security skills development, students should pursue courses in any order as seats become available through their national points of contact.

Individual course highlights

Each course lasts 10 weeks and is offered twice per year. Each begins with one week of in-residence instruction at NSO in Germany, followed by eight weeks of facilitated distance learning, culminating with a final week in residence for student evaluation and graduation. The course list includes:

- M6-108 Network Security Course, the introductory course, is offered in collaboration with the U.S. Partnership Training and Education Center in Monterey. This course forms the bedrock of the program, which prepares graduates to comprehend the bits-in-transit aspect of network security. Foundational topics include defining networks, exploring routers, routing and access-control-list basics, traffic analysis, perimeter defense, e-authentication and virtual private network protocols.
- M6-109 Network Vulnerability Assessment Course complements and expounds upon M6-108 fundamentals. It aims to arm graduates with methodologies and techniques required for vulnerability assessments and follow-on mitigation. These methodologies are reviewed in-depth and are applied from the vantage point of hackers attempting to analyze and exploit common vulnerabilities. The course also uses lab exercises to solidify understanding of security threats, weaknesses and emerging methods of exploitation.
- M6-110 Cyber Incident Handling and Disaster Recovery Planning Course logically follows M6-109, stressing comprehension of the nature and scope of cyber-security-incident handling services, such as policy, planning, operations and technology issues. Students gain insight into intrusion/incident detection, minimizing loss of service, service continuity, and forensic analysis and service/data restoration. Ultimately, students learn how to mitigate and respond to natural disasters, denial of service, malicious code, malicious misuse of hardware and firmware, unauthorized access, data compromise and inappropriate use of network equipment.
- M6-111 Network Traffic Analysis Course completes the four-course cyber security program. By design, this course is the most robust. It not only supplements previous academics, it integrates real-time practical analysis and evaluation — the ultimate challenge. Students are expected to master operation of protocol/traffic analyzing equipment while simultaneously reviewing, analyzing and evaluating either "live" or prerecorded network traffic for indications and/or forensic evidence of potential, impending or realized configuration errors or malicious attacks.

Key allies and partners can expect powerful strategic and operational cyber security training programs, whether through NSO or the Marshall Center, to shape future engagements well into the future.

Conclusion

Whether NSO's popular cyber security courses are pursued individually or part of the recommended complete package, graduates glean invaluable cyber-awareness acumen in a critically functional area. As cyber threats continue to evolve, NSO will counter them by fortifying and adapting its strategies.

Meanwhile, the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany, is planning to launch its own tailored cyber security program in the summer of 2014 with possible plans to collaborate with NSO.

Key allies and partners can expect powerful strategic and operational cyber security training programs, whether through NSO or the Marshall Center, to shape future engagements well into the future. □