BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

CYBER-PHYSICAL SYSTEMS AND CRITICAL INFRASTRUCTURE

HIGHLIGHTING NORTHROP GRUMMAN CORPORATION'S WORK

Cyber-Physical Systems and Critical Infrastructure: Highlighting Northrop Grumman Corporation's Work

AS COMPUTERS BECOME EVER FASTER AND BANDWIDTH EVER CHEAPER, computing and communication capabilities are being embedded within more and more objects and structures in the physical environment. Engineered systems, which bridge the cyber world of computing and communications with the physical world, are called cyber-physical systems (CPS). Recognizing the need to secure CPS both nationally and statewide, Virginia has developed a world-leading technology ecosystem founded on private industry innovation and public-private partnership. This publication highlights Northrop Grumman Corporation's (Northrop Grumman) work in Virginia at the intersection of cyber-physical systems and critical infrastructure.

THE CHALLENGE

Northrop Grumman's efforts in critical infrastructure are driven by its external and internal customer needs. Its core customers have awakened to the seriousness of cyber threats that affect not only the protection of information but also potentially the systems that interact with our "physical world." Issues such as lack of patch management, outdated operating systems, weak authentication, and user error expose critical infrastructure entities to cyber threats from malicious actors, including nation-states. In addition, as the number of "connected" devices continues to grow, an overwhelming number of end-points will touch both the virtual and physical worlds. The volume, variety, and velocity of these devices will be a challenge to any organization to effectively integrate and defend within their infrastructures.

THE SOLUTION

Northrop Grumman maintains a robust cybersecurity capability through leading-edge technology and one of the most advanced workforces in the nation. It leverages and incorporates the best practices from across industry and government into its efforts, including those from the SANS Institute and the National Institute of Standards and Technology (NIST). It also collaborates with several organizations in the development and operation of its cybersecurity solutions such as NIST with respect to its National Initiative for Cybersecurity Education and Risk Management Framework. In addition, Northrop Grumman leverages the robust set of higher education institutions within Virginia to build its workforce. Northrop Grumman's highly skilled workforce, robust internal research and development program, and partnership with government and academia make its approach to cybersecurity comprehensive.

In 2014, the Department of Homeland Security (DHS) awarded Northrop Grumman a five-year contract to support the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). As part of that work, Northrop Grumman's government contractors handle incidents by notifying victims of

cyber threats, providing mitigation measures, and working with asset owners/operators to improve awareness. The ICS-CERT provides critical infrastructure entities in the private and public sectors with mitigation strategies and incident response services that are tailored to the sector and the entity's needs. In addition to DHS, Northrop Grumman works with the Federal Bureau of Investigation, the U.S. Intelligence Community, the Information Sharing and Analysis Centers, the Department of Energy's National Labs, and other government agencies on the ICS-CERT contract.

Over time, the ICS-CERT has reported and mitigated a growing number of incidents. An emerging challenge in victim notification is a lack of awareness of the ICS-CERT as a legitimate organization that can provide assistance and support. It is important for the nation's critical infrastructure entities to be aware that such services are available to help them secure critical infrastructure, especially during potentially catastrophic cyber attacks from nation-states.

RECOMMENDATIONS

At a high level, data analytics, electrical engineering, computer science, computer engineering, and systems engineering are the skills needed in the area of cyber-physical systems and critical infrastructure. The workforce will need workers with knowledge of industrial control systems and cybersecurity as well as managers and executives who can listen and react to information from asset owners/operators. Thus, the nation should pursue an interdisciplinary approach to educating the next-generation workforce that will be at the forefront of cyber-physical systems and the challenges associated with their integration.

All organizations need to invest in infrastructure to protect themselves from cyber threats. In some cases, recovery from an attack is far costlier than mitigation would have been. As the world becomes more connected, it will be important for organizations to share information such as mitigation strategies with others in their sector to increase situational awareness. Leaders should consider the risks of every decision, whether it be related to configuration, implementation, execution, or operation of systems that are part of critical infrastructure. It is necessary to begin building a strategic plan now, with respect to how cyber-physical systems will impact specific organizations. The need for a skilled workforce and advanced capabilities will continue for cybersecurity and, more specifically, cyber-physical systems for the near future. By making cyber issues a priority, Virginia serves as an outstanding leader in enabling these efforts to occur.

STAFF CONTACT

Mr. Christopher Valentino
Director of Joint Cyberspace Programs
Cyber & Intelligence Mission Solutions Division
Northrop Grumman Mission Systems
christopher.valentino@ngc.com

ADDITIONAL INFORMATION

https://ics-cert.us-cert.gov

"Northrop Grumman is raising awareness of the services that are available to secure critical infrastructure from potentially disastrous cyber attacks. Supported by Virginia's world-leading technology ecosystem, Northrop Grumman's work in this area succeeds through its highly skilled workforce, robust internal research and development program, and partnerships with government, industry, and academia."

CHRISTOPHER VALENTINO / DIRECTOR OF JOINT CYBERSPACE PROGRAMS, CYBER & INTELLIGENCE MISSION SOLUTIONS DIVISION / NORTHROP GRUMMAN MISSION SYSTEMS

ABOUT THE BUSINESS-HIGHER EDUCATION FORUM

The Business-Higher Education Forum (BHEF) is the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the creation of a highly skilled future workforce. BHEF members collaborate and form strategic partnerships to build new undergraduate pathways; improve alignment between higher education and the workforce; and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

ABOUT NORTHROP GRUMMAN CORPORATION

Northrop Grumman Corporation (Northrop Grumman) is a leader in providing cybersecurity solutions to its customers and protecting internal infrastructure. Within Virginia, Northrop Grumman's highly skilled workforce supports both government and internal customers from its locations in McLean, Falls Church, and Fair Lakes. In critical infrastructure, Northrop Grumman manages a Department of Homeland Security contract to support the Industrial Control Systems Cyber Emergency Response Team.

ACKNOWLEDGEMENTS

BHEF would like to thank Christopher Valentino and Vincent Harris for providing detailed information on Northrop Grumman's work in critical infrastructure. BHEF would also like to thank the National Governors Association and the Office of Naval Research for their contributions and support.

This work is funded by the Center for Innovative Technology and the National Science Foundation under Award DUE-1331063.

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

2025 M Street NW, Suite 800, Washington, DC 20036

202.367.1189 / info@bhef.com / www.bhef.com