
© Peach ShutterStock/Shutterstock.com

Security Convergence for Air and Space Power

XX

Resilience in Three Dimensions

By Col Dr Eric Trias, US Air Force, and
Col Martin Rothrock, US Air Force
Defense Threat Reduction Agency

Introduction

Looking to the future, the commander of Allied Air Command called for increased efforts to achieve MDO – Multi-Domain Air and Space Operations.[1] Although one of the goals of MDO is to increase resiliency, our reliance on technology to achieve multi-domain operations Command and Control (C2) without a corresponding focus on protection will increase the fragility of critical infrastructure vital to Air and Space (A&S) operations, against enemies developing their own multi-domain capabilities with lethal hybrid warfare strategies. Moreover, threats to A&S operations are becoming increasingly complex as state actor adversaries develop their own multi-domain capabilities not only to physically attack defence critical infrastructure through cyber means, but also to exploit vulnerability of information systems to gain physical access. A promising approach for NATO to assure operations resiliency in the face of this multi-domain threat lies in the concept of convergence of three

security disciplines – physical, cyber, and Continuity of Operations (COOP). NATO can no longer depend on cybersecurity alone for operational resiliency, nor can the Alliance rely entirely on guards, guns, and gates to protect critical missions, people, and infrastructure. Comprehensive risk-managed operational practices complemented by diverse, converged security protection programs are needed to meet the challenge.

Why Security Convergence?

Commercial businesses have begun to realize the benefits of converging physical and cyber protection disciplines. A commercial industry survey reports that among Chief Security Officers of worldwide commercial firms with converged physical security and cybersecurity operations, 78 % reported significant benefits to the effectiveness of their security posture.[2] Additionally, commercial industries view convergence of cyber and physical security with COOP, a.k.a. business continuity in industry, as synergistic and highly beneficial. The concept creates an effective response to both natural hazards and manmade threats while creating an effective resiliency posture ensuring mission continuation as a response to both cyber and physical incidents delivering a three-dimensional defence-in-depth protection.

Although physical security has long been deemed essential to preventing unauthorized physical access to critical equipment, assets, or facilities, physical security is often overlooked as vital to protecting all potential access vectors to critical information systems, such as servers or workstations located outside key facilities. Just as effective physical security programs prevent theft, these programs must extend throughout the architecture to prevent data exfiltration or modification by unauthorized users. Gaining physical access to any information system renders even the best cybersecurity measures ineffective, e.g., keyloggers can be planted, systems can be booted surreptitiously using a compromised operating

system, or side-channel analysis can be conducted to bypass cryptographic protection. Often critical cyber terrain infrastructure's primary means of protection is through isolation from other networks. However, this 'air-gapped' protection scheme does not guarantee immunity from physical attack, as illustrated by the well-known attack on Iran's Natanz Nuclear Facility by an insider delivering the STUXNET malware through a USB device.[3]

Equally neglected is the perspective of employing cybersecurity to protect modern physical security technology systems is necessary. Evolution of physical security systems transitions proprietary electronic security systems to rely on Internet Protocol (IP)-based architecture as part of the Internet of Things (IoT) technology.[4] IP-based intrusion detection systems along with access and circulation control systems have become increasingly effective and affordable options to protect A&S operations instead of robust military or contracted security forces. However, these systems continue to suffer from widespread vulnerability to cyber threats including weak password practices, poorly protected credentials, improper configuration management, and many even had built-in vulnerabilities which have allowed outsiders to take full control of cameras systems to conduct espionage or utilize them to gain surreptitious access to other networked systems.[5]

Most importantly, security convergence establishes collaboration among the protection disciplines to more effectively defeat the same threats.[6] Consequently, cybersecurity systems and physical security systems (riding on the same network) should employ similar risk management processes and practices. These disciplines both rely on threat assessment, access control, continuous monitoring and rapid response to incidents. As a result, converging security incident response and C2, while using parallel risk management practices, of physical and cybersecurity systems, can more effectively address, prevent, and mitigate potential incidents through predictive analysis.[7]

How to Achieve Convergence Using Risk Management?

In 2020, according to an IBM research, the average cost of a data breach globally and in the US were $3.86 M and $8.64 M, respectively.[8] Even with strong motivations to mitigate risks to address these costs, the global security industry has been slow to eliminate barriers between security disciplines and adopt the concept of convergence. These barriers are likely to be even more difficult for NATO to overcome given the need to achieve consensus among 30 nations. Progress will take time and deliberate effort. However, pragmatic objectives presented here lay out a roadmap for convergence achievable in the next five years. Along the way, utilizing the existing NATO Force Protection (FP) model provides an excellent framework for guiding convergence of cybersecurity, physical security, and COOP programs through a comprehensive risk management process.[9]

The first objective is to improve overall COOP readiness. COOP bridges the gaps between physical security, emergency response, and cybersecurity and provides the greatest improvement of mission resilience for a comparatively modest investment in training and resources. The first step in the NATO FP model, ***mission analysis***, provides the basis for developing more effective COOP to support NATO A&S missions. This process results in identification of the most important assets to accomplish the mission and develops understanding of associated Mission Essential Functions (MEFs) or critical capabilities these assets perform. The resilience against multi-domain attacks can be achieved through establishing redundancy of these capabilities, dispersing physical assets, building alternative procedures, and/or separating mission systems (or critical portions of these systems) from vulnerable networks.

Multiple natural disasters have demonstrated the value of an effective COOP program. However, as the frequency of cyber-attacks increase, organizations must include response to cyber-attacks into their COOP programs. As an example, in 2017, Denmark's Maersk, the world's largest

shipping company, became a victim to the NotPetya ransomware devastating its information systems worldwide. Maersk was only able to reconstitute its network, without paying the ransom, due to a fortuitous power outage at an office in Accra, Ghana. Due to the prolonged power outage, the servers were offline when the infected software update propagated throughout Maersk's 108 office in 34 countries. Maersk was able to rebuild its data and administrative systems by physically transporting the Ghana hard drives to the company's headquarters.[10] Although, this specific incident response enabled successful reconstitution of operations, it illustrates the need for an effective COOP process not based on good luck.

The next objective to achieve convergence is to broaden the NATO FP risk management process to embrace a multi-domain approach. Threat assessment, vulnerability assessment, and the risk mitigation responses emerging from this process must be developed through a converged perspective. Broadening the threat assessment aperture is particularly important for NATO because the Alliance faces a hybrid threat increasing in speed, scale, and intensity that combines kinetic attacks from irregular forces with cyber-attacks. However, it won't be easy! NATO faces significant challenges in sharing threat information among Alliance stakeholders and in achieving agreement on threat prioritization, not only due to the 30 nations represented, but just as significantly, to the limited interaction that traditionally exists in military organizations between communications/cyberspace and physical security communities. Additionally, cyber threat information is often classified at a level where it cannot be shared easily among national intelligence services. Nevertheless, NATO must address these challenges to support converged protection of operations. Additionally, use of multi-domain red teams to demonstrate vulnerabilities and development of a Design Basis Threat (DBT) outlining expected adversary cyber, intelligence gathering, and kinetic capabilities can be helpful to achieve consensus on how to robust a security system needs to be and what it is intended to protect against. The NATO FP vulnerability assessment, if conducted with a

broader view of multi-domain threats, will inform commanders to consider how both physical and cyber threats can be paired to exploit critical assets to achieve the greatest consequences against their missions. It will show commanders where best to apply multi-domain security resources to achieve a converged defence against hybrid threats.

The NATO threats and hazards identification process identifies the most severe risks to the mission along with countermeasures to consider for reducing risk to an acceptable level. A good example of how this can work for NATO in security convergence is to consider a data centre. In addition to cybersecurity configuration controls and monitoring systems, a data centre supporting an A&S C2 role needs strong physical protections with access control systems, CCTVs, guards, advanced fire protection systems, and redundant utilities for heating and cooling. The ultimate insurance policy for the data centre is a robust, executable COOP plan to answer key questions: Can the alternate site take over all, or part, of the centre's capabilities? Can the MEF's be reconstituted quickly in an alternate location before significant impact occurs? Has the COOP plan been rehearsed? Do adequate resources exist to execute it? When conducting multi-domain A&S operations in a contested environment, these issues are likely to be more important than simply tracking weapon system availability.

Conclusion: The Strategic Challenge

Strengthening COOP and building a multi-domain risk assessment process will get NATO on the road towards dealing with current and future hybrid threats. However, a strategic approach is needed to position NATO to stay ahead of emerging threats. One strategic challenge on the road to convergence is to expand the multi-domain risk assessment model 'outside the wire,' to include assessment of the physical protection, cyber protection, and business continuity programs of commercial infrastructure

vital to A&S missions. Another strategic objective, involving changing organizational cultures, is to build a converged mindset among NATO protection professionals in security, cybersecurity, and emergency response disciplines. This can be best accomplished by creating integrated protection units, where personnel are required to train and exercise together to apply their respective disciplines to assure a common mission. Lastly, leadership commitment and championing will be required, along with the support and buy-in of dedicated security professionals.

Convergence shows promise and has been achieved by many large commercial enterprises.[11] It will take deliberate strategy and policies to ensure progress and true convergence occur in NATO. Government organizations and commercial industry must share best practices among stakeholders to expedite adoption and normalization of this security paradigm. The benefits of achieving a three-dimensional security converged environment for mission assurance in a contested multi-domain environment are substantial now, and it will be even more critical in the future to ensure the success of NATO A&S multi-domain operations.

Colonel Eric D. Trias (US Air Force), PhD, is Chief of the Cyber Division, at the Defense Threat Reduction Agency, Nuclear Enterprise Directorate, Mission Assurance Department. He leads all Cyberspace related mission assurance activities in support of Joint Staff directives and DoD assessments of its most critical assets.

Colonel Martin L. Rothrock (US Air Force) is the Chief of the Joint Mission Assurance Assessments Division for the Defense Threat Reduction Agency at Fort Belvoir, Virginia. Col Rothrock is a career Security Forces officer who has commanded at the Squadron, Group, and Wing level.

Endnotes

1. Harrigian, Jeffrey L., 'Shaping the Future Multi-Domain C2', JAPCC Journal, Ed. 29 (2020), p. 6–8.
2. Beck, D., Gips, M., and Pierce, B. M., The State of Security Convergence in the United States, Europe, and India, Alexandria: ASIS International, 2019.
3. Greenberg, A., Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, New York: Doubleday, 2019.
4. Ibid. 2.
5. Bugeja, J., Jonsson, D., and Jacobsson, A., 'An Investigation of Vulnerabilities in Smart Connected Cameras,' IEEE International Conference on Pervasive Computing and Communications Workshops, Athens: 2018, p. 537–542.
6. Ibid. 2.
7. Ibid. 2.
8. IBM Security, 'Cost of a Data Breach Report 2020,' https://www.ibm.com/security/digital-assets/cost-data-breach-report, accessed 26 Jan. 2021.
9. NATO AJP 3.14., 'Allied Joint Doctrine for Force Protection', Apr. 2015, p. 3–6.
10. Ibid. 3., p. 103.
11. Ibid. 2.