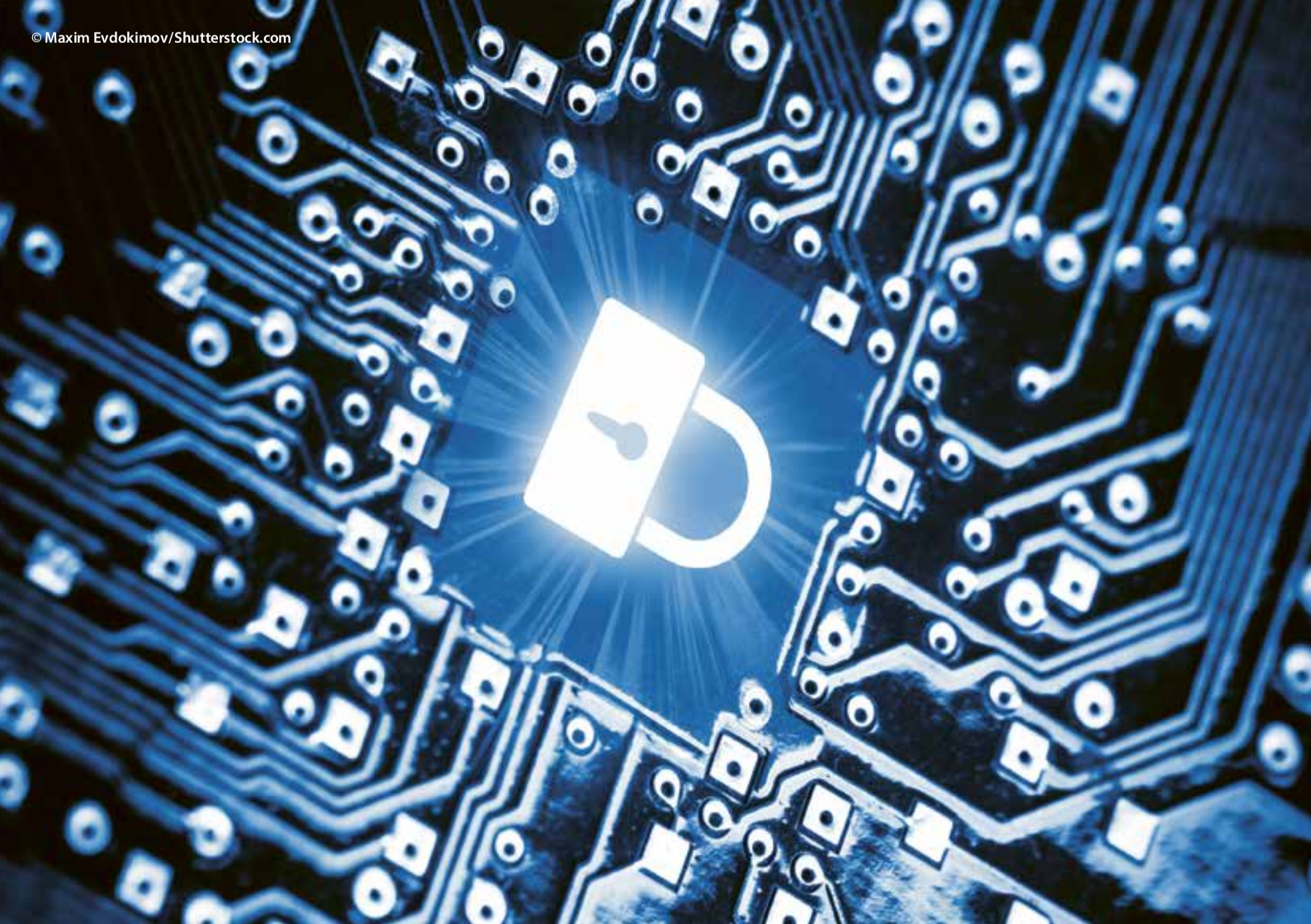
© Maxim Evdokimov/Shutterstock.com

Cyberspace and Joint Air and Space Power

XVII

Any Speed; Always Relevant

By Lt Col Paul J. MacKenzie, CA Air Force
Joint Air Power Competence Centre

Introduction

When examining the Cyberspace Domain where the projection of Air and Space power is concerned, it is just as relevant for mission success to maximize the defence of systems and information throughout the slow and arduous process of aerospace project delivery, as it is during the rapid and time-sensitive coordination and execution of Air and Space operations. This paper will outline the relevance of considering Cyberspace, and cybersecurity in particular, from the earliest slow-moving stages of Air and Space systems Research and Development (R&D), and how activities in these phases can eventually influence the Air and Space power capability gaps with potential adversaries. The paper will also discuss the importance of a secure and reliable cyber-network through to the opposite end of the Air and Space power spectrum, from mission planning and the publication and distribution of orders, to the fast-paced execution and coordination of Air and Space operations to deliver Air and Space power with precise timing and accuracy.

Research and Development

Considering the earliest stages of Air and Space Power capability delivery, with modern systems inextricably dependent on the information technology, operating systems, and applications that comprise the physical and logical layers of the Cyberspace domain, aerospace systems are vulnerable to exploitation from adversaries. The vulnerabilities are present from the early stages of R&D through to when systems are delivered. Adversaries will find or create and exploit vulnerabilities throughout the slow and laborious program delivery period in order to reduce the capability gap, exploiting the weakness in cyber defences to impede the effectiveness of NATO forces while working to improve that of their own. Industrial espionage of military programs via Cyberspace has been stated to be part of what represents one of the largest transitions of wealth in human history.[1] China, for example, is reported to have stolen, and continues to steal, data on US stealth fighters, engines, radars and missiles.[2] This data will have been leveraged to influence improvements in the design, production, and performance of their systems and assist in their reconnaissance (and possibly exploitation) of vulnerabilities in allied systems. The 2020 attack on the SolarWinds business software,[3] impacting thousands of government, public, and private organizations globally, is recent evidence of the ongoing vulnerability and threat to industry and, inevitably, the military which relies upon it.[4]

Strategic Planning to Mission Execution

The shrinking capability gap and loss of advantage presents many challenges as this impacts strategy and mission planning, influences decisions regarding orders of battle, risk assessment, estimating potential success rates and many other factors for Air and Space operations. Considering the actual execution of Air and Space operations, the integration

and coordination of resources of multiple domains in time and space is essential for mission success, so securing the cyber-network across which this coordination takes place is paramount. As all nations enhance their capabilities, Cyberspace is an increasingly contested environment. Achieving supremacy in Cyberspace in this era, against a peer or near-peer adversary, is unlikely; superiority is more achievable. Still, claiming only superiority recognizes that the enemy has a vote and can influence the Cyberspace domain to some degree. What is critical to understand is that, in modern operations, freedom of manoeuvre in Cyberspace will be challenged, so superiority is not permanent but temporary. This is extremely relevant when Air and Space capabilities, as well as those in other domains, in multi- or all-domain operations, are integrated with Cyberspace and brought to bear against an adversary. In such operations, mission success hinges on the skilful coordination and management of resources and on the availability of systems, in and through Cyberspace, being assured. This integration is exemplified by recent engagements coordinated by Combat Controllers (CCT) during operations in Afghanistan. The CCTs employed a variety of communications (PRC 177F and MBITR Radios),[5] to communicate with multiple aircraft (F-18 Fighter/Bombers, AC-130 Gun Ships, E3 Airborne Warning and Control [AWACS], E-8 JSTARS, P-3 Orions, Predator UAS, AH 64 Apache Attack and CH 47 Chinook Transport Helicopters) and multi-service special operations forces on the ground (Navy Seals, Rangers, Delta Force operators, Air CCTs). They coordinated flying and ground movement, managing airspace using several systems (Falcon View digital mapping, deployable navigational beacons, portable Global Positioning System (GPS)) while directing a variety of ordnance (Blu-118/B 2000n thermobaric laser-guided bombs, JDAMS) for precise and overwhelming effect.[6, 7] All of these systems, when digitally interconnected to establish a larger system, lethal as it was, had myriad attack surfaces with varying degrees of vulnerability to attack in and through Cyberspace, which introduced greater risk to the mission. Fortunately, at the time these missions were executed, with this

arrangement of forward command and control, Allies enjoyed at least superiority, if not supremacy, over the enemy in Cyberspace. Consequently, the aggregate results were achieved with optimum speed and relevance with respect to delivery of Air and Space power. Historically speaking, the combination resulted in 'one of the deadliest and least known forces in the history of human warfare.'[8] The degree of success realized in these missions, however, hinged on the confidentiality, availability, and integrity of information and the systems operating in real-time in the Cyberspace domain, a condition that will be challenged in the future by potential peer and near-peer adversaries.

Defence

The defence and resilience of the Cyberspace domain is critical to mission success. NATO relies on the NATO Communications and Information Agency (NCIA) to defend its own Cyberspace links and nodes. Contributing nations have agreed, through the Cyber Defence Pledge, to ensure the resources they force generate for NATO have been provided sufficient cybersecurity.[9] Honouring this pledge requires each nation to implement programs to provide the maximum level of security. For example, the United States is implementing a Zero Trust Architecture (ZTA)[10] for Federal Agencies to enhance security and has adopted the Cybersecurity Maturity Model Certification as part of multiple lines of effort focused on the security and resiliency of their Defense Industrial Base in order to enhance the protection of the supply chain.[11]

It is vital that Cybersecurity be achieved to the greatest extent possible, though it is understood that it is impossible to protect systems completely. In the course of Air and Space operations, 'system components vary in importance to a mission, and this importance can change throughout the life of a mission'.[12] Consequently, 'these systems' risks to the Air mis-

sion from Cyberspace need to be identified, managed, and monitored throughout the life of the mission.'[13] Despite the very best efforts, systems may be degraded by adversary action in and through Cyberspace. Therefore 'the Air domain might need to carry out critical mission activities using vulnerable parts of Cyberspace simply because it has no alternative.'[14] Indeed, the 2017 Annual Report of the US Director, Operational Test and Evaluation (DOT&E) highlighted that 'although directed by The Chairman of the Joint Chiefs of Staff in 2011 and endorsed by two subsequent Secretaries of Defense, DOT&E has not observed many demonstrations that Commands can 'fight through' a major cyber-attack and sustain their critical missions.'[15] On the degree of difficulty scale of measures to adapt to cybersecurity threats, exercising in a degraded environment should be considered easier relative to most measures and be high on the list of priorities, particularly when considering the possible consequences of being unprepared.

Offense

NATO, as a defensive Alliance, does not possess offensive Cyberspace capabilities of its own. However, this does not preclude a commander from exploiting offensive capabilities when offered voluntarily by Allies. Still, coordinating offensive Cyberspace operations so they are executed at the speed of relevance particularly when in concert with other components in Joint All Domain Operations is a highly complex endeavour. 'The timing and sequencing of joint operations has always presented unique challenges, cyber adds a new dimension.'[16] In reality, it takes a great deal of time to plan and progress through the steps necessary to produce effects in/through Cyberspace, steps collectively referred to as the Cyber Kill Chain. Some attack surfaces and/or vulnerabilities that the planning would aim to exploit may have changed before the weapon is deployed, which means many possible vulnerabilities will need to be found, or even

created, in order to increase the likelihood of success. That said, 'once a system is exploited, the effects of a cyber-attack can be nearly instantaneous.'[17] In such circumstances, where the success of a joint mission is dependent on the success of a Cyberspace operation, it would be necessary to design the payload with a trigger to coincide with the correct conditions to exist for allied conventional forces, such as a time, traffic pattern, or message content on an adversary's network.

Future

To be able to operate in the Cyberspace domain at the speed of relevance in the future NATO must successfully exploit emerging trends and technologies. Close cooperation is required between governments, industry, academia, and the military. From a defensive perspective, NATO's potential adversaries are automating their attacks, which means NATO must 'use the same kind of automation and artificial intelligence and machine learning to counter those attacks.'[18] This includes using AI 'to identify and mitigate zero-day cyber-attacks and advanced persistent threats.'[19] The same technologies will be leveraged, in a similar but opposite fashion, to identify and help create vulnerabilities for use in offensive Cyberspace operations. Advanced technologies are, according to the Chief Scientist for the US Government Accountability Office, 'a double edge sword'[20] the more we employ the more vulnerable we become. The objective is to optimize the advantages and reduce the disadvantages. AI and quantum computing, 'each of these is a massive, disruptive technology … (and) what makes each even more powerful is their convergence … These are linked by cyber; either as a core competency or in a vital supporting role.'[21] Further into the future are the possibilities of controlling technologies via brain-to-machine interfaces. The promise of this possibility has been made more realistic based on recent work with implants coated with a polymer that facilitates the interface between synthetic materials that have an electronic

charge in solid-state, and biological tissue that has an ionic charge in a wet state.[22] Our ability to exploit this and similar advances in technology will help to increase the speed of transforming operational intent into effect.

Conclusion

If NATO is to continue to achieve success, protecting systems and information from attacks in and through Cyberspace, while at the same time exploiting the advantages the domain provides, must be a core requirement going forward. Cyberspace must be at the forefront in consideration from the early stages in force development through to force generation and employment. As with all domains, it is imperative NATO outpace and outinnovate its potential adversaries if it is to reach the speed and operational tempo required to generate effects and achieve the technological advantage, if not outright superiority, necessary to be an effective military instrument of power at the speed relevance in the NATO warfighting concept.

Lieutenant Colonel Paul J. MacKenzie (CA Air Force) MSM (US), CD. A Communications and Electronics Engineering (Air) Officer in the Royal Canadian Air Force, he examines Cyberspace as it relates to NATO Joint Air and Space Power and from a defensive perspective through to the potential in exploiting offensive effects. He holds a Master's of Science degree in Computer and Information Technology (System Engineering), is a graduate of the Canadian Forces Joint Command and Staff Program and has over 32 years of experience in the provision of IT/CIS to operations.

Endnotes

1. Flannery, Russell, 'China Theft of U.S. Information, IP one of the Largest Wealth Transfers in History: FBI Chief' (published online 7 Jul. 2020), https://www.forbes.com/sites/russellflannery/ 2020/07/07/china-theft-of-us-information-ip-one-of-largest-wealth-transfers-in-history-fbi-chief/ ?sh=27b060834440, accessed 24 Jan. 2021.
2. Carlin, John, Dawn of the Code War, Public Affairs, 2018, p. 274–275.
3. Brewster, Thomas, 'DHS, DOJ and DOD Are All Customers of SolarWinds Orion, The Source of the Huge US Government Hack' (published online 14 Dec. 2020), https://www.forbes.com /sites/ thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=7785505d25e6, accessed 19 Jan. 2021.
4. The attack itself involved the use of a Trojan Horse on IT Monitoring and Management software, enabling creation of a back door and subsequently permitting lateral movement and data theft. The malware was sufficiently sophisticated to permit evasion from detection and to obscure its actions once it had successfully compromised the system by masquerading as a legitimate improvement program protocol.
5. Army Navy Portable Radio communications (AN/PRC) 117F: A multiband, man-portable, tactical, software-defined combat-net radio with embedded communications security, satellite communications, and electronic countermeasures. AN/PRC -148 Multiband Inter/Intra Team Radio (MBITR): A multiband, handheld, tactical, software-defined radio, widely used by NATO forces around the world.
6. Schilling, Dan, and Chapman Longfritz, Lori, 'Alone at Dawn – Medal of Honor Recipient John Chapman and the Untold Story of the World's Deadliest Operations Force', Hachette Book Group, Inc., 2019.
7. Naylor, S., Relentless Strike, The Secret History of Joint Special Operations Command, St. Martin's Press, 2015.
8. Ibid. 4., p. 9.
9. NATO, 'NATO Cyber Defence Pledge', 8 Jul. 2016, https://www.nato.int/cps/en/ <natohq/ official_texts_133177.htm, accessed 28 Jan. 2021.
10. Rose, S. W., Borchert, O., Mitchell, S., and Connelly, S., Zero Trust Architecture, NIST Special Publication 800-207, US Department of Commerce, 2020.
11. Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory, 'Cybersecurity Maturity Model Certification (CMMC)' Version 1.02, 18 Mar 2020.
12. Cummins, James, 'The Challenges of Cyber Freedom of Manoeuvre For Airpower in the Information Age', Joint Services Command and Staff College, (2020): p. 12.
13. Ibid. 10., p. 18.
14. Ibid. 10., p. 19.
15. US Director Operational Test and Evaluation, 'FY 2017 Annual Report', Jan. 2018, p. 319.
16. McArdle, Jennifer, 'Victory Over and Across Domains – Training for Tomorrow's Battlefields', Center for Strategic and Budgetary Assessments, 2019, p. 41.
17. Ibid. 14., p. 42.
18. Seffers, George I., 'DISA, JAIC Developing AI-Enabled Cybersecurity Tool – Automation is the key to keeping up with adversaries', SIGNAL, Dec. 2020, p. 16.
19. Ibid. 16., p. 17.
20. Ackerman, Robert K., 'A Cyber Thread Runs Through Government Future Assessments', SIGNAL, Oct. 2020, p. 31.
21. Ibid. 18.
22. Seffers, George I., 'The Brain-to-Machine Interface Just Became Better', SIGNAL, Dec. 2020, p. 38.