U.S. Navy Cmdr. Charles Elliott, Cyber Coalition 2022 exercise director, briefs participants during Cyber Coalition 2022 in Tallinn, Estonia. NATO's Allied Command Transformation-led exercise tested and trained cyber defenders from across the alliance on their ability to defend NATO and national cyber networks. (Photo courtesy of NATO)

NATO's Cyber Era (1999–2024)

Implications for Multidomain Operations

Melia Pfannenstiel, PhD

Dan Cox, PhD

Following NATO's seventy-eight-day air campaign (24 March–10 June 1999) to halt ethnic violence in Kosovo, U.S. Air Force Gen. John P. Jumper remarked, "Instead of sitting and talking about great big large pods that bash electrons, we should be talking about microchips that manipulate electrons and get into the heart and soul of systems like the SA-10 or the SA-12 and tell it that it is a refrigerator and not a radar."[1] While the United States tested offensive cyber capabilities by neutralizing Serbian air defenses, Operation Allied Force marked the first cyberattack against the NATO alliance. Following the May 1999 accidental bombing of the Chinese embassy in Belgrade, activists sympathetic to Russia, Serbia, and China targeted the Supreme Headquarters Allied Powers Europe and U.S. military websites in defacement and dedicated denial of service attacks.[2]

Through the experience of Operation Allied Force and a growing awareness of cyber threats, NATO established the Cyber Defense Program during the 2002 Prague Summit to advance its deterrence and defense mission.[3] However, it was the relatively simple but devastating cyberattack on NATO member Estonia's government, media, and banking systems in April–May 2007 that marked a critical juncture in cybersecurity. The cyberattack followed Estonia's decision to relocate a Soviet-era statue, which sparked riots and looting by Russian-speaking Estonians. On the second night of riots, botnet-delivered spam and online requests from Russian IP addresses overwhelmed public and private servers. The dedicated denial of service attack created panic and chaos, as government officials struggled to communicate, the media could not transmit accurate information, and Estonians were unable to complete banking transactions.[4]

Much of the disruption in Estonia lasted days, but the event transformed NATO's understanding of effects created through the cyber domain, and the role of cybersecurity within the alliance's deterrence and defense posture. This article further examines the context surrounding the 2007 attack, the evolution of NATO cyber defense efforts, such as the Tallinn-based Cooperative Cyber Defense Center of Excellence (CCDCOE), and NATO's campaign of learning from Russia's persistent cyberattacks on Ukraine since 2013. The final section reviews the importance of the cyber domain in 2024, as NATO looks to future multidomain operations (MDO).

The 2007 Cyberattack on Estonia

Russia's interest in hacking may be traced to the 1980s, when a small group of hackers based in West Germany approached East German officials with an offer to steal information from Western governments and sell it to the Soviet KGB. The classic book on cybersecurity, *The Cuckoo's Egg*, provides an account of the attempt to penetrate U.S. organizations, such as the Department of Defense, White Sands Missile Range, and NASA's Jet Propulsion Laboratory. A decade later, during a warming of U.S.-Russia relations, the United States began detecting intrusions into its government systems. In what became known as Moonlight Maze, between 1996 and 1999, the United States investigated a series of intrusions on national security-related entities. Following a Russian military official's disclosure to U.S. officials in early 1999 that Russian intelligence was responsible, the cyber espionage activities paused before escalating with greater sophistication.[5] Beginning in late 1998, the U.S. Department of Defense (DOD) launched a series of joint task forces to organize offensive and defensive cyber operations, including computer network defense, computer network operations, global network operations, and the joint functional component command-network warfare.[6]

The 1990s marked a period of strategic ambiguity for the NATO alliance. The collapse of the Soviet Union and dissolution of the Warsaw Pact in 1991 left NATO's purpose unclear, as its primary role since 1949 was collective defense against Soviet expansionism. Russia began expressing its discontent

Melia Pfannenstiel, PhD, is an associate professor of social science at the U.S. Army School of Advanced Military Studies, Fort Leavenworth, Kansas. She received her PhD in security studies from Kansas State University. She has previously published on terrorism, disinformation, and cyber warfare.

Dan Cox, PhD, is a professor of political science at the U.S. Army School of Advanced Military Studies, Fort Leavenworth, Kansas. He received his PhD in political science from the University of Nebraska. He has also served in the NATO Partnership for Peace Program. His current research interests are cybersecurity, disinformation, future warfare, and design and complexity theory. He is also researching Chinese and Russian warfare.

with NATO enlargement in 1991, and despite repeated claims by Russia, no formal agreements placed geographic limits on NATO membership. By 1995, NATO pursued a path for enlargement, specifically for former Warsaw Pact members and post-Soviet Republics. Poland, Hungary, and the Czech Republic (now Czechia) joined NATO in March 1999, weeks before the start of Operation Allied Force. During the 1999 Washington Summit in April, NATO announced an expanded strategic vision and established membership action plans for aspiring members, including the Baltic states.[7]

The Baltic states of Latvia, Lithuania, and Estonia pursued similar paths following the Soviet collapse. Each distanced itself from Russia and joined NATO in 2004.[8] Bringing NATO to Russia's border triggered longstanding fears from the thirteenth-century Mongol invasion, the Napoleonic era wars, and the German invasion during World War II. NATO expansionism also weakened the Russian strategic initiative of buffer states to protect its long border.[9]

Meanwhile, Russian diaspora communities perceived the domestic policies of Baltic states as discriminatory.[10] Following Estonian independence in 1992, ethnic Russian residents assumed a stateless status, as they were unable to apply for dual citizenship and the Estonian government delayed granting them citizenship. Many Russian residents became "gray passport" holders, leaving domestic and international legal issues unresolved.[11]

By 2007, domestic policies left Russian residents with fewer education and employment opportunities and earning less than Estonians.[12] Estonia's nation-building included the controversial decision to transfer a bronze Soviet statue and World War II soldier graves, known as the "Monument to the Liberators of Tallinn," to a cemetery outside the city center.[13] Amid perceptions that the Russian diaspora were victims facing further dishonor of Soviet memory, Vladimir Putin's speech at the Munich Security Conference on 10 February 2007 harshly criticized NATO expansion for bringing insecurity to Russia and the world.[14]

While Russians viewed the Tallinn memorial as marking liberation from the Nazis, many Estonians viewed it as a reminder of Soviet occupation. As work to move the statue began on 26 April 2007, protests turned to violent confrontations with police. During the outbreak of riots, Russian-language media fueled outrage through false claims about Estonian plans to destroy the monument.[15]

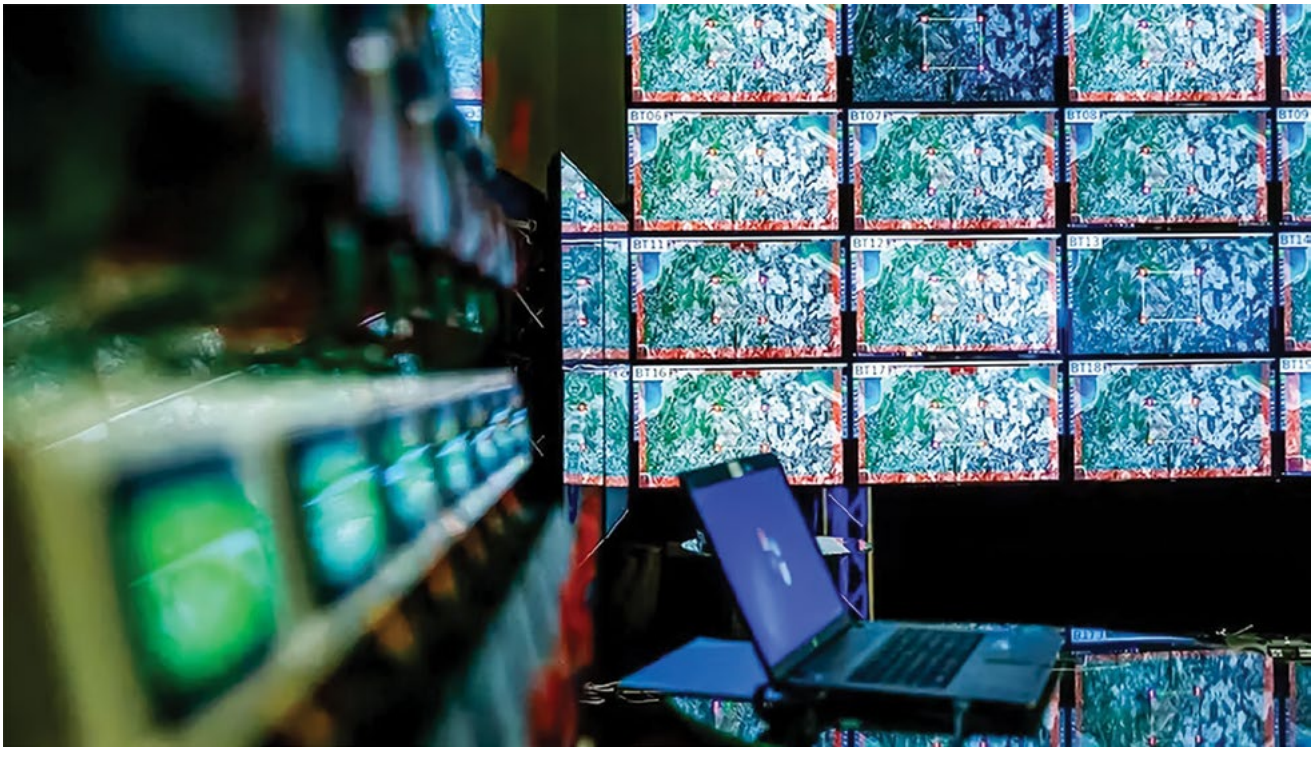
Aside from Russian media amplifying the grievances of Russian-speaking Estonians, Russia also suspended contracts with Estonian firms and cut rail transit.[16] Internet sites in Estonia began experiencing disruptions in the early morning hours of 27 April 2007. Estonian Defense Minister Jaak Aaviksoo noticed interruptions to prominent news websites and governmental sites. As one of the most wired countries in the world and an early adopter of an e-government system, Estonia was uniquely vulnerable to such an attack.[17]

Throughout the attacks, banks and ATMs were unable to complete transactions for hours at a time.[18] The initial attacks were unsophisticated but appeared coordinated to produce confusion and a lack of confidence in the government and the banking system. The Estonian government recovered from the first wave of attacks within days by blocking foreign access to the domestic Estonian internet, but two days of chaos resulted in over one thousand arrested or detained, 156 injuries, and one fatality.[19]

Following a brief lull, online discussions indicated plans for a second wave of attacks to coincide with Russia's Victory Day on 9 May, which commemorates Soviet sacrifices and the defeat of Nazi Germany in World War II. To rally patriotic Russian hackers, one online discussion referred to "eSStonia," in suggesting Estonian government ties to Nazis. The wave of attacks beginning on 8 May 2007 appeared more coordinated and sophisticated than the April attacks in exploiting vulnerabilities, but Estonia adapted to each attack.[20]

The collective circumstances surrounding the attack led cybersecurity professionals to believe Russian sympathizers and the Russian state likely coordinated resources and activities. Without clear attribution, NATO chose not to invoke Articles 4 or 5 of the Washington Treaty. Later dubbed "Web War I," the 2007 attack highlights ambiguity and surprise across domains and dimensions.[21]

The attack also represents an iteration of arranging diplomatic and economic activities, cyber domain effects, and human and informational dimensions. During the summer of 2008, Russian aggression against Georgia, a non-NATO member, marked its first use of



The soon-to-be-established NATO Integrated Cyber Defence Centre will enhance the protection of NATO and allied networks and the use of cyberspace as an operational domain. The center will inform NATO military commanders of possible threats and vulnerabilities in cyberspace, including those to critical privately owned infrastructure necessary to support military activities. (Photo courtesy of NATO)

cyberattacks synchronized with a conventional military operation across land, air, and maritime domains.[22]

NATO's Coming of Age in the Cyber Domain

NATO's 2002 Cyber Defense Program initiated collective security measures through the NATO Computer Incident Response Capability. The NATO Computer Incident Response Capability formed the first iteration of a team for cyber incident prevention, detection, and response. Following the 2007 Estonia experience, the 2008 Bucharest Summit established "the need for NATO and nations to protect key information systems; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyberattack," along with a Cyber Defense Management Authority and Cyber Defense Management Board to coordinate cyber defense throughout NATO civilian and military institutions, and formation of the CCDCOE.

In October 2008, NATO officially accredited the CCDCOE as an international military organization to be based in Tallinn to strengthen cyber defense capabilities and coordinate responses to future cyberattacks. The CCDCOE is not centered on a cyber operations mission, although it formed rapid response teams, but instead, its mission focuses on doctrine development, training, and education to build interoperability and coordinate capability sharing among alliance members and partners.[23]

Following its establishment, the CCDCOE invited legal scholars to produce a manual for the relevant norms and laws governing cyberwarfare. Drawing broad expertise from academics, legal practitioners, technicians, and representatives from NATO's Allied Command Transformation, U.S. Cyber Command, and the International Committee of the Red Cross, the initial *Tallinn Manual* relied on existing interpretations regulating the conduct of armed conflict, including the law of armed conflict or international humanitarian law addressing means in warfare such as landmines, electronic warfare, and the ban on disrupting food and water to noncombatants.[24]

Operation Unified Protector, the 2011 intervention to protect civilians in Libya, demonstrated the alliance's capacity for defending against cyberattacks. During the planning and execution of air operations

in Libya, NATO approved a comprehensive approach to cyber defense. The 2011 action plan emphasized the protection of NATO systems and established an intent to share training and expertise beyond member states to alliance partners, other international organizations, and academia. Aside from increasing funding and elevating the priority of cyber defense initiatives, NATO strengthened and expanded its cyber defense exercises through the CCDCOE. Recurring exercises such as Cyber Coalition and Locked Shields are foundational in building interoperability and sharing capabilities across alliance members and partners.[25]

NATO'S Cyber Lessons from Ukraine (2013–2024)

Among the assumptions held by Russia and many in the West regarding how a large-scale invasion of Ukraine would unfold, one common belief was that "shock-and-awe" Russian cyberattacks would cripple Ukrainian infrastructure and defenses. Following Russia's 2022 invasion, some observers noted an unprecedented number of cyberattacks, while various others refer to their seemingly minimal strategic impact as the cyber "dog that didn't bark."[26]

Since 2013, Russia consistently targeted the Ukrainian population through information and influence operations, cyber espionage, and the disruption and destruction of governmental sites, telecommunications, and critical infrastructure in attacks through the cyber domain. An onslaught of various operations began alongside the late 2013 EuroMaidan demonstrations that prompted the removal of Ukraine's pro-Russian President Victor Yanukovich from power in 2014. Russia promoted various narratives to Ukrainian audiences ranging from their shared history, culture, and traditions to the victimization of Russian speakers in Ukraine or accusations that Ukraine is sympathetic to Nazism.[27]

Anger surrounding Ukraine's pivot to the West and growing relationships with NATO countries by the spring of 2014 fueled Russia's aggression. A prevailing theme in Russia's strategic approach is "sub threshold" activities, including information warfare and cyber operations, which may be further categorized as "cyber technical" and "cyber psychological."[28] In the lead up to the 2014 stealth invasion and occupation of Crimea and the Donbas, Russia used the internet as a medium for information operations to sow confusion and garner support among Russian speakers. Russia engaged in a series of attacks to facilitate conventional ground operations.[29]

Russia coordinated cyber, electronic warfare, and information operations, including the use of cellular phones, as early as 2014.[30] On 11 July 2014, at Zelenopillya, Ukraine, Russian-backed forces attacked and destroyed over two battalions of vehicles, killing thirty soldiers, and injuring over a hundred, in a matter of minutes. Preceding this rapid devastation, Russian-backed groups disrupted lines of communication, while cell phone data from soldiers in tightly packed assembly areas allowed Russian forces to target Ukrainians with artillery and drones.[31]

By late 2014, efforts to manage Russian hostilities in Ukraine did not stop its escalation of cyber and information operations. Private industry and Western governments identified cyber reconnaissance activities on critical infrastructure but gained a clearer understanding of intentions in 2015–2016 during a flurry of offensive strikes. Russia began more sophisticated cyberattacks on Ukraine's critical infrastructure, often timed with other military activities. By early 2017, attacks on media, energy, transportation, and finance affected the Ukrainian government, military, and civilian population. As a NATO official focusing on cybersecurity noted at the time, "You can't really find a space in Ukraine where there *hasn't* been an attack … Turn over every rock and you'll find a computer network operation."[32]

The June 2017 NotPetya malware, considered "the most destructive cyberattack in history," affected approximately 10 percent of computers in Ukraine, including hospitals, banks, airports, and government agencies, in addition to spreading across dozens of countries and disrupting global shipping networks.[33] The vast economic damage caused of NotPetya, which targeted Ukraine but spread globally, occurred within months of the WannaCry malware and drove ongoing discussions within NATO over attribution and responses.[34]

While not a member of the alliance, Ukraine's relationship with NATO provided mutually beneficial capacity building, through programs and CCDCOE exercises to share information and strengthen defenses. Ukraine became the largest beneficiary of NATO's Science for Peace and Security programs in 2014, but a

Seized computer hardware is displayed after law enforcement officials exposed a million-dollar pro-Russian bot farm in Ukraine on 2 August 2022. Members of the organized criminal group spread misinformation on the internet about the activities of the country's top military and political leadership. (Photo courtesy of the Ministry of Internal Affairs of Ukraine via Wikimedia Commons)

July 2017 NATO-Ukraine working group meeting addressed ongoing cooperation on critical security issues such as cyber defense.[35]

Alongside learning from Ukraine's experience, cyber threats to NATO members increased in 2016–2021. NATO pursued several ways to strengthen its deterrence and defense posture. In December 2016, NATO and the European Union formalized forty measures for greater cooperation, followed in February 2017 by NATO defense ministers approving an updated Cyber Defense Action Plan and roadmap for cyber as a domain of operations. The July 2018 NATO Summit in Brussels established the Cyberspace Operations Center alongside a new command structure to enhance military situational awareness, specifying NATO operations and missions may draw from member nation cyber capabilities, but "Allies maintain full ownership of those contributions, just as Allies own the tanks, ships and aircraft in NATO operations and missions."[36] NATO published *Allied Joint Doctrine for Cyberspace Operations* in 2020, for planning, execution, and assessment of operations. Despite recorded reservations, doctrine offers a common language for "federated" systems used in missions.[37] In September 2021, NATO appointed a chief information officer to better integrate information and communications technology.[38]

Ukraine strengthened its relationship with NATO countries through a series of exercises in 2021, as Russia signaled its intent to escalate the war it began in 2014.[39] By late 2021, hackers began developing malware that was later deployed in the days leading up to Russia's full-scale invasion of Ukraine on 24 February 2022. Cyberattacks, either on behalf of or sympathetic to Russia, targeted Ukraine's government, banking, energy, media, education, information technology, and agriculture sectors, communications infrastructure, and logistics networks assisting refugees fleeing the conflict. The widespread and numerous cyberattacks lacked notable strategic effect and appeared poorly coordinated with Russian conventional military operations. However, Ukrainian efforts to strengthen cyber

defense in cooperation with a network of partners since 2014 likely denied Russia's ability to execute cyber and information operations synchronized with conventional military operations, "suggesting that a well-prepared and energetic defense can have the advantage over offense in cyberspace."[40]

On the CCDCOE's fifteenth anniversary in 2023, Ukraine became an official contributing member, along with three other non-NATO members.[41] In late December 2023, nine NATO alliance members formalized the Tallinn Mechanism to coordinate and facilitate civilian cyber assistance to Ukraine.[42]

Ukraine and international partners continually mount a strong cyber defense and improve information sharing and interoperability. Russia also demonstrates a propensity to learn and adapt through the ongoing conflict and cyberattacks to date may have a compounding or emergent effect not yet realized. Claims of the cyber "dog that didn't bark" also highlight the complexity of planning cyber operations within a campaign, as synchronizing effects and measuring effectiveness may differ from other domains.[43]

While too soon to draw conclusions in the cyber offense-defense debate from the ongoing Russia-Ukraine war, for NATO's deterrence and defensive posture, initial lessons underscore the importance of a strong, adaptive network of cyber defenders to deny information advantage to an adversary. Russia's ongoing campaign in Ukraine continues to unify the alliance on the importance of cyber defense. Cyberattacks on member governments or infrastructure, particularly a months-long cyberattack on NATO member Albania in 2022, drive ongoing discussions on the threshold for attribution and the future of offensive cyber operations. NATO maintains a policy of strategic ambiguity on the threshold for a cyberattack initiating Article 5 to maintain alliance cohesiveness and flexibility in planning for contingencies.[44]

NATO's Transition to Multidomain Operations

NATO adopted the AirLand Battle concept developed in the United States to support its defense and deterrence posture during the Cold War, but strategic ambiguity and rapid technological innovation during the 1990s fostered thinking about the future of warfare.[45] During Operation Allied Force in 1999, NATO members realized the potential risk of not protecting computer-enabled systems, but also the potential opportunities in developing new cognitive approaches and technical capabilities to enable maneuver in the air domain.[46] Network-centric and systems approaches gained wider acceptance in military discourse.[47]

The 11 September 2001 terrorist attacks on the United States prompted NATO to invoke Article 5 for the first time and focus on the threat from violent extremist organizations. NATO militaries reframed their thinking from conventional militaries toward a counterinsurgency and counterterrorism focus on Afghanistan. U.S. allies and partners tested new information, cyber, and electronic warfare capabilities, particularly against the Islamic State, by the mid-2010s. The global environment was shifting to strategic competition during this time, and the United States began to turn its attention to building on these cyber capabilities and developing concepts better suited for high-intensity conflict.[48]

By 2016, the U.S. military began actively developing the concept of MDO. Recognizing the general idea behind MDO was not new, dialogue focused on the interdependence between domains and the importance of networks across the cyber/electromagnetic spectrum and space domains that enabled synchronization.[49] "Straddling all five warfighting domains, cyberspace is not merely the connector of all systems, but also a weapons platform in itself" as MDO calls for synchronizing activities across domains to present "multiple dilemmas" to an adversary's decision-making.[50]

Developments within the United States such as the U.S. Army's 2018 concept for MDO coincided with NATO organizational changes for cyber operations. The CCDCOE continued to develop its education and training focus to strengthen interoperability; the alliance announced the formation of a cyberspace operations center in Brussels and continued developing doctrine for cyber operations.[51]

Between 2022 and 2023, the alliance formally pursued MDO as a strategic priority. The *Alliance Concept for Multi-Domain Operations* presented in March 2023 defined MDO as the "orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance."[52]

The contributions of individual alliance members vary as of 2024, but cyber-related lessons from the war

A Ukrainian servicewoman learns to operate a first-person view drone in the Zaporizhzhia region of Ukraine. Unmanned aircraft have become an integral part of Russia's war against Ukraine. (Photo by Elena Tita via the collection of https://war.ukraine.ua/)

in Ukraine continue to inform NATO's concept of MDO. Among these lessons is leveraging military and commercial capabilities for sensing, communications redundancy, cyber defense, command and control, fires, and unmanned aircraft systems.[53]

As Gen. John P. Jumper envisioned in 1999, electromagnetic spectrum and cyber capabilities present options for the suppression of enemy air defenses (SEAD) mission.[54] Success in SEAD missions is vital for MDO, as it enables ground maneuver. Russia's inadequate SEAD is one aspect of failure in Ukraine. NATO members should learn from such observations and pursue creative ways to build resiliency within systems and develop capabilities to enable access and maneuver across domains.[55]

Conclusion

NATO began dialogue to establish organizations, systems, and processes after its first experience with cyberattacks in 1999. Operation Allied Force may be viewed as an antecedent to the critical juncture in NATO cybersecurity—the 2007 attacks on Estonia. The Estonia attacks previewed a pattern of Russian subthreshold information and influence activities through the cyber domain. Since the founding of the CCDCOE in 2008, NATO is better prepared to continually learn and adapt to these evolving threats. Despite success in partnering with Ukraine to strengthen its resiliency to Russian cyberattacks, NATO members and partners face evolving threats beyond Russia.

Cyber defense is an enduring requirement for MDO, as it enables critical capabilities such as command and control, information, sustainment, and fires. Continued development of NATO's cyberspace operations center can provide commanders with situational awareness and decision advantage that presents competitors with multiple dilemmas. CCDCOE research and education, exercises, and doctrinal development facilitate common language and interoperability in MDO. The expanse of the cyber domain presents unique vulnerabilities, but the specialized knowledge and expertise within NATO allows for protection and redundancy in and across distributed systems.

Seventy-five years after its founding, NATO maintains its defense and deterrence posture with reinvigorated purpose. Underpinning collective defense and deterrence, the expanding network of allies and partners requires the continual refinement of a warfighting concept, systems, and doctrine to develop combat-credible forces capable of conducting MDO. As NATO looks to the future, maintaining networked connectivity through the electromagnetic spectrum and cyber domain are central to advancing the alliance's mission. ■

Notes

1. Benjamin S. Lambeth, *NATO's Air War in Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001), 112, https://www.rand.org/pubs/monograph_reports/MR1365.html.

2. Jason Healy and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" (Washington, DC: Brookings Institution, September 2014), 2, https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf.

3. Ibid., 1.

4. Damien McGuiness, "How a Cyber Attack Transformed Estonia," BBC, 27 April 2017, https://www.bbc.com/news/39655415.

5. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), 72–76.

6. Melia Pfannenstiel, "USCYBERCOM," in *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology*, ed. Nicholas Sambaluk (Santa Barbara, CA: ABC-CLIO, 2019), 109–11.

7. Paul Gallis, *NATO: Congress Addresses Expansion of the Alliance*, Congressional Research Service (CRS) No. RL30192 (Washington, DC: CRS, 24 May 1999), 6–10, 15–16, https://www.everycrsreport.com/files/19990524_RL30192_c9adab6ad1b595a94d0196df7cc4e54710bb28e1.pdf.

8. McGuiness, "How a Cyber Attack Transformed Estonia."

9. Glenn Kessler, "NATO Seeks to Soothe Russia," *Washington Post* (website), 3 April 2004, https://www.washingtonpost.com/archive/politics/2004/04/03/nato-seeks-to-soothe-russia/2c46ac29-1b42-4121-8fc8-3fdf8302ee40/.

10. "Ethnic Russians in the Baltics," Stratfor, 21 May 2014, https://worldview.stratfor.com/article/ethnic-russians-baltics.

11. Tacita Vero, "The Gray Zone," Slate, 13 March 2017, https://slate.com/news-and-politics/2017/03/many-ethnic-russians-in-estonia-have-gray-passports-live-in-legal-limbo.html.

12. Epp Kallaste, "Significant Pay Gap between Estonians and 'Non-Nationals,'" Eurofound, 18 March 2007, https://www.eurofound.europa.eu/en/resources/article/2007/significant-pay-gap-between-estonians-and-non-nationals.

13. Greenberg, *Sandworm*, 80.

14. Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security*, ed. Dan Remenyi (Reading, UK: Academic Publishing Limited, 2008), 163–68, https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

15. McGuinness, "How a Cyber Attack Transformed Estonia."

16. Piret Pernik, "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine," in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, ed. Nicu Popescu and Stanislav Secrieru, Chaillot Paper No. 148 (Paris: European Union Institute for Security Studies, October 2018), 54, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

17. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian* (website), 16 May 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

18. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired* (website), 21 August 2007, https://www.wired.com/2007/08/ff-estonia/.

19. Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

20. Greenberg, *Sandworm*, 84.

21. Ibid., 87–88.

22. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 155.

23. Healy and Jordan, "NATO's Cyber Capabilities," 1–2.

24. Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 7–10.

25. Ibid.

26. Healy and Jordan, "NATO's Cyber Capabilities," 3–4.

27. Jaclyn A. Kerr, *Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons* (Arlington, VA: Center for Naval Analysis, November 2023), 2, https://www.cna.org/reports/2023/11/Assessing-Russian-Cyber-and-Information-Warfare-in-Ukraine.pdf.

28. Ibid., 7–9.

29. Rod Thorton and Marina Miron, "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking," *Cyber Defense Review* 7, no 3 (Summer 2022): 118–19.

30. Donghui Park and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," Henry M. Jackson School of International Studies, 11 October 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

31. Alan Yuhas, Thomas Gibbons-Neff, and Yousur Al-Hlou, "For Russian Troops, Cellphone Use Is a Persistent, Lethal Danger," *New York Times* (website), 4 January 2023, https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html.

32. Amos Fox, "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield," Modern War Institute, 17 January 2017, https://mwi.westpoint.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/.

33. Greenberg, *Sandworm*, 26–27, 47.

34. Buchanan, *The Hacker and the State*, 300–1.

35. "NotPetya and WannaCry Call for a Joint Response from International Community," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 30 June 2017, https://ccdcoe.

org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/.

36. "NATO Boosts Cooperation with Ukraine on Scientific and Security-Related Activities," NATO, last updated 6 July 2017, https://www.nato.int/cps/en/natohq/news_145789.htm.

37. "Cyber Defence," NATO, last updated 30 July 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm.

38. Allied Joint Publication-3.20, *Allied Joint Doctrine for Cyberspace Operations*, Edition A, Version 1 (Brussels: NATO Standardization Office, January 2020), 2, https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

39. NATO, "Cyber Defence."

40. "Ukraine Holds Military Drills with U.S. Forces, NATO Allies," Reuters, 20 September 2021, https://www.reuters.com/business/aerospace-defense/ukraine-holds-military-drills-with-us-forces-nato-allies-2021-09-20/.

41. James Andrew Lewis, *Cyber War and Ukraine* (Washington, DC: Center for Strategic and International Studies, 16 June 2022), 1–2, 11–12, https://www.csis.org/analysis/cyber-war-and-ukraine.

42. "The NATO CCDCOE Welcomes New Members Iceland, Ireland, Japan, and Ukraine," NATO Cooperative Cyber Defence Centre of Excellence, 17 May 2023, https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/.

43. Office of the Spokesperson, "Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine," U.S. Department of State press release, 20 December 2023, https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/.

44. Kerr, "Assessing Russian Cyber and Information Warfare in Ukraine," 2, 5–9.

45. Sarah Wiedemar, "NATO and Article 5 in Cyberspace," *CSS Analysis in Security Policy* 323 (Zürich: Center for Security Studies at ETH Zürich, May 2023), 1–4, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf.

46. Lambeth, *NATO's Air War in Kosovo*, 223–34, 246–47; James Black and Alice Lynch, "Cyber Threats to NATO from a Multi-Domain Perspective," in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, ed. A. Ertan et al. (Tallinn, EE: NATO CCDCOE Publications, 2020), 126–50, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

47. Chairman of the Joint Chiefs of Staff, *Joint Vision 2020: America's Military—Preparing for Tomorrow* (Washington, DC: Joint Chiefs of Staff, June 2000), https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CB-0CB942-1274110898250/aledc_ref/joint_vision_2020.pdf.

48. Franz-Stefan Gady and Alexander Stronell, "Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030," in Ertan et al., *Cyber Threats and NATO 2030*, 151–77.

49. Jeffrey Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air and Space Power Journal* 30, no. 1 (Spring 2016): 60–71, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf.

50. Gady and Stronell, "Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030," 152.

51. Black and Lynch, "Cyber Threats to NATO from a Multi-Domain Perspective," 126–30.

52. Franklin D. Kramer, Ann M. Dailey, and Joslyn A. Brodfuehrer, "NATO Multidomain Operations Near- and Medium-Term Priority Initiatives" (Washington, DC: Atlantic Council, 21 February 2024), 5, https://www.atlanticcouncil.org/wp-content/uploads/2024/03/NATO-multidomain-operations-Near-and-medium-term-priority-initiatives.pdf.

53. Ibid., 8–9.

54. Lambeth, *NATO's Air War in Kosovo*, 102–12.

55. Kramer, Dailey, and Brodfuehrer, "NATO Multidomain Operations Near- and Medium-Term Priority Initiatives," 12–13.

US ISSN 0026-4148