Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency
NATO COE-DAT Handbook 1

Carol V. Evans
Editor

Contributors

In 2014, NATO’s Center of Excellence-Defence Against Terrorism (COE-DAT) launched the inaugural course on “Critical Infrastructure Protection Against Terrorist Attacks.” As the CIPTA course garnered increased attendance and interest, the core lecturer team felt the need to update the course in critical infrastructure (CI), taking into account the shift from an emphasis on “protection” of CI assets to “security and resiliency.” What was lacking in the fields of academe and emergency management and the industry practitioner community was a handbook that leveraged the collective subject-matter expertise of the core lecturer team, a handbook that could serve to educate government leaders, state and private-sector owners and operators of critical infrastructure, academicians, and policymakers in NATO and partner countries. Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency is the culmination of such an effort, the first major collaborative research project under a Memorandum of Understanding between the US Army War College, Strategic Studies Institute (SSI), and NATO COE-DAT.

The research project began in October 2020 with a series of four workshops hosted by SSI. The draft chapters for the book were completed in late January 2022. Little did the research team envision the Russian invasion of Ukraine in February this year. The Russian occupation of the Zaporizhzhya nuclear power plant, successive missile attacks against Ukraine’s electric generation and distribution facilities, rail transport, and cyberattacks against almost every sector of the country’s critical infrastructure have been on world display. Russian use of its gas supplies as a means of economic warfare against Europe—designed to undermine NATO unity and support for Ukraine—is another timely example of why adversaries, nation-states, and terrorists alike target critical infrastructure. Hence the
need for public-private sector partnerships to secure that infrastructure and build the resiliency to sustain it when attacked. Ukraine also highlights the need for NATO allies to understand where vulnerabilities exist in host-nation infrastructure that will undermine collective defense and give more urgency to redressing and mitigating those fissures.

The conceptual framework for this handbook addresses key aspects of which users need to have a baseline knowledge. What is critical infrastructure and why is it important for NATO and an individual nation’s security? Threats and attacks to CI may occur from many vectors, including kinetic attacks conducted largely by terrorists to cyberattacks by terrorists, nation-states, and their proxies, to hybrid threats. Among the many critical infrastructure sectors, there are designated lifelines, ones that are vital due to their importance to the well-being of society, the continuity of government operations, economic impacts, and the deleterious, cascading effects on other CI sectors. There has been a recent shift in the critical infrastructure community of practitioners from an emphasis on merely the protection of key vital infrastructure assets to building in security and resilience of that infrastructure. What then are the tools that nation states and owners and operators of CI can employ to achieve these twin goals?

To provide an understanding of these important CI topics, SSI and COE-DAT brought together leading international experts. This multidisciplinary team consisted of industry practitioners, US and European policymakers, members from the intelligence community, research laboratory experts, and academicians. Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency consists of three major sections. The first section includes four chapters that focus on what we mean by “critical” infrastructure and why and how it has been targeted. There has been an evolution of physical attacks, mainly by terrorists, to sophisticated cyberattacks by adversaries and to more complex hybrid means. Chapter 1, “Understanding Critical Infrastructure,” by Ron Bearse sets the stage for the book by answering the following questions: What is critical infrastructure? Why is it important? What is the difference between critical infrastructure protection (CIP) and critical infrastructure security and resilience (CISR)? What is involved in implementing CISR policy in and across the North Atlantic Treaty Organization nations? Bearse suggests that CISR is a quintessential societal task for maintaining national security, economic vitality, and public health and safety in a world filled with increasing levels of risk. For NATO member states, building and enhancing CISR at the national level is necessary to safeguard societies, people, and shared values and also provide the foundation for credible deterrence and collective defense.

Chapter 2, “Physical Threats to Critical Infrastructure,” by Malcolm Baker, Ronald Bearse, and Ray Mey details kinetic threats to CI by terrorists with a useful case study regarding the 2013 attack by an al-Qaeda affiliate on the Amenas oil and gas facility in Algeria. They also examine natural and other physical threats
to infrastructure, as well as future man-made threats that are of greatest concern to NATO, including chemical, biological, radiological, nuclear, explosive (CBRNE) devices, drones and unmanned aerial vehicles, precision strike weapons, and an electromagnetic pulse attack.

Chapter 3, “Cyber Threats to Critical Infrastructure,” by Salih Biçakci examines how risks against critical infrastructure are on the rise in the cyber domain. He writes that while the COVID-19 pandemic has compelled businesses to adopt practices to accommodate a more remote workforce, it has also presented malevolent attackers an unprecedented opportunity to test cybersecurity systems and exploit vulnerabilities. The pandemic has demonstrated the need for the dependable and continuous operation of electricity, natural gas, oil, water and wastewater systems, and telecommunications. His chapter provides an overview of a critical infrastructure’s technical layers and systems and its potential organizational vulnerabilities to cyberattacks related to the human workforce and management. He highlights the various categories of threat actors (opportunistic attackers, competitors, insider threats, advanced persistent threats, and hacktivists) and concludes with an overview of recent primary attack types that threat actors employ to exploit vulnerabilities in critical infrastructure.

The fourth and last chapter in section one is “Hybrid Threats to US and NATO Critical Infrastructure” by Carol V. Evans. She provides an analysis of several major hybrid threat vectors to critical infrastructure with the potential to attack, undermine, or compromise US and NATO warfighting, force projection, and sustainment capabilities. The first threat vector is the deliberate cyber infiltration by adversaries of the energy infrastructure that supports US installations and bases. This infiltration enables adversaries to interfere with the US military’s ability to deploy and sustain forward combat forces and equipment. A second hybrid threat vector is adversarial targeting of US and NATO logistics, with the potential to degrade US overseas force projection as well as NATO mobility and sustainment within the theater. The third hybrid threat stems from China’s strategic penetration, ownership, and control of key defense industrial-base infrastructure and supply chains in Europe via its Belt and Road Initiative and foreign direct-investment activities. This vector provides an opportunity to undermine US and NATO interoperability and political unity. Dr. Evans’s chapter concludes by highlighting US and NATO measures to redress and mitigate these threats by investing in CISR through organizational capacity building, development of policy frameworks, and the implementation of host country baseline resilience requirements.

The second section centers on giving readers an appreciation of the critical “lifeline” infrastructure sectors, namely, energy and transport (including civil aviation and mass transit rail), water, and communications. Leading this section is Chapter 5, “European Energy and the Case of Ukraine,” by Theresa Sabonis-Helf. Written prior to the Russian invasion of Ukraine in February 2022, Dr. Sabonis-Helf posits that potential
electricity interruption in the West is becoming both increasingly catastrophic for urbanized areas and more attractive to threat actors seeking disruption. The avenues for disruption are becoming greater as energy systems become larger, “smarter,” and more internationally linked. The intertwined relationship between electricity security and cybersecurity calls for an understanding of CISR that recognizes both sets of vulnerabilities. Dr. Sabonis-Helf argues that the case of Ukraine is thus instructive. Ukraine’s experience of energy security and cybersecurity reveals significant risks and offers insight into NATO’s efforts to enhance civil preparedness and collective CISR among Allies and partners. It also illustrates the complexities that Ukraine and Europe are facing today and will face in the future.

Chapter 6, “Civil Aviation,” by David Harell analyzes the aviation infrastructure sector and the threats it faces, including primary aircraft bombings and ground attacks on airports by terrorists. To understand the civil aviation sector, he writes it is important to know why the aviation industry is so critical, what makes it so volatile, and why it is such an attractive target for terrorists. He provides several key reasons for the industry’s vulnerability: its rigidity, its predictability, and its difficulty in keeping up with evolving terrorist threats. Harell uses multiple case studies—which span the 20 years after the 9/11 attacks—to illustrate these vulnerabilities. He also examines the aviation security responses to these terrorist attacks and identifies important lessons to be learned. He concludes with recommendations and best practices that can assist in reducing the vulnerabilities across international civil aviation.

Chapter 7, “Mass Transit Railway Operations,” by Adrian Dwyer explains the inherent vulnerability of open transport networks, such as railway operations, to terrorist action. He showcases those methods of attack that have often been used, drawing on case study data from Great Britain, continental Europe, the United States, Japan, and India. From the perspective of NATO, the targeting of rail networks across its member states can disrupt military logistics, the civilian supply chain, and economic prosperity more generally. Dwyer maintains that strategic risk assessment is an important means to manage diverse terrorist threats and inherent vulnerabilities of mass rail transit.

Chapter 8, “Water Sector Resilience and the Metropolitan Washington Case,” by Steve Bieber provides an eye-opening analysis of how fragile the supply of this vital resource can be and how other sectors of critical infrastructure are highly dependent on water. Bieber identifies the risks and threats to the water sector; outlines key steps in resilience planning; illustrates challenges and solutions to security and resilience initiatives using a case study from Washington, DC; and offers recommendations for developing water-sector security and resilience. He explains that the security and resilience of the water sector is a key enabler of a nation’s civil preparedness, with military implications as well. Terrorist threats to water delivery or contamination of water sources can impact a nation’s ability to move and sustain its military forces and project military power
when required. From the perspective of the North Atlantic Treaty Organization, threats to the water sector in one member state could have ripple effects that limit or diminish NATO’s military mobility and force projection in support of its essential core tasks.

Chris Anderson’s Chapter 9, “Communications Resilience,” completes the handbook’s second section on the lifeline CI sectors. Communications form the critical backbone of the modern world, and resilient and trustworthy communications are fundamental to national security and emergency preparedness. Communications play many critical roles for NATO, he writes, including: command and control, military operations, distribution of intelligence and warning signals, crisis management and coordination, and citizen preparedness. Anderson provides an in-depth overview of the communications sector and explains the ways in which the integrity, availability, or confidentiality of communications systems may be degraded or compromised. He shows the risks to the communications sector using recent natural, man-made, cyber, and kinetic incidents that have impacted communications systems and related infrastructure. He provides important recommendations for improving communications resilience against terrorist attacks and other threats.

The third section of Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency provides readers and users of the handbook with the tools necessary to deter and mitigate attacks against critical infrastructure as well as the means to build long-term security and resiliency within host-nation infrastructure, thereby enabling NATO’s collective defense. There are six chapters in this section. It begins with Chapter 10 by Ron Bearse and Alessandro Lazari, who employ their respective policy-making purviews to collaborate on “Comparing Policy Frameworks: CISR in the United States and the European Union.” The US and EU CISR policies and practices are the most advanced frameworks in the world, and many countries have emulated the US and EU models. Their chapter describes the key underpinnings and characteristics of each respective policy framework, the reasons why these frameworks came into being, and how they were adapted over time. The intent of this chapter is to help Allies and partners better understand these two CISR policy frameworks so they can apply the key principles and tenets to enhance the CISR posture in their respective countries.

In Chapter 11, “Information and Intelligence Sharing,” Chris Anderson and Raymond Mey discuss the important role of information and intelligence sharing between governments and state or private sector owner-operators of critical infrastructure. These activities are essential to the success of any CISR effort across the North Atlantic Treaty Organization. They explain that key infrastructure stakeholders need to share information to understand comprehensive infrastructure risk so they can then determine the most efficient and effective means to mitigate these dangers. This process involves building trust,
shared and practiced communications methods, and structured, multidimensional information sharing. Anderson and Mey provide some best practices of public-private information-sharing programs from the United States. These practices include the Department of Homeland Security Critical Infrastructure Partnership Advisory Council (DHS CIPAC), Protected Critical Infrastructure Information (PCII) program, Cyber Information Sharing and Collaboration Program, as well as the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF), the Domestic Security Alliance Council (DSAC), and InfraGard. One information-sharing program common in the United States and Europe is an Information Sharing and Analysis Center (ISAC), which is a critical infrastructure sector-specific organization to share information about threats and vulnerabilities.

Chapter 12, “Critical Infrastructure Interdependency Modeling and Analysis: Enhancing Resilience Management Strategies,” by Duane Verner provides a tour-de-force overview of the need for NATO member states and partner nations to understand infrastructure interdependencies since they operate in concert with each other. Catastrophic events can cascade across these interconnected systems and hamper the ability of critical infrastructure operators to remain operational. Modeling and analysis of these interdependencies are key components to an effective risk-management strategy and to determining where resources are needed to build resiliency. Verner summarizes general approaches to model and assess critical infrastructure, and he proposes a flexible CISR framework to inform the development of resilience management strategies. NATO Allies and partners can use this framework to reduce the risks posed to critical infrastructure and to foster greater resilience through cross-sector collaboration.

How NATO can best manage and assess security risk in a constantly changing environment is the starting point for Geoffrey French’s Chapter 13 on “Security Risk Assessment and Management.” As he points out, organizations and communities need formal processes to determine, prioritize, and address risks. The promise of risk management is that with sufficient uniformity and consistency, government or private-sector leaders can make better decisions through the ability to aggregate risks at different levels. His chapter explores in depth the concepts of risk assessment and risk management and reviews a set of selected risk-management frameworks—from the International Organization for Standardization (ISO), NATO, US Government Accountability Office (GAO), and the US National Infrastructure Protection Plan (NIPP)—that have been designed or adapted for security risk management. French then demonstrates how a national-level governmental risk program can encourage and guide risk-management practices as well as coordinate the constellation of public- and private-sector organizations involved in critical infrastructure operations to foster a mutually supportive environment for CISR.

While Biçakci’s earlier chapter describes the various cyber threats to CI, Sungbaek Cho provides users of this handbook with some important cybersecurity tools to mitigate those very threats. In Chapter 14,
“Enhancing Cybersecurity of Industrial Control Systems,” Cho offers a brief overview of the characteristics of industrial control systems (ICSs) and why they are subject to cyberattacks in terms of the vulnerability of the components as well as the prevalent practice in modern critical infrastructure to operate ICS in more open interconnections with business networks. He highlights these vulnerabilities with some major cyber event case studies, including: Stuxnet (2010), BlackEnergy (2011), Ukraine Blackout (2015), RWE’s Nuclear Power Plant in Germany (2016), TRITON (2017), and the Colonial Pipeline (2021). The chapter offers best practices and tools for critical infrastructure stakeholders, owners, and operators to protect their systems and enhance security and resilience against cyberattacks. Cho recommends the utilization of risk-management methodologies, basic hygiene practices, and essential cybersecurity measures. Although NATO is taking steps to improve its collective ability to defend against and respond to cyberattacks against Allied critical infrastructure, individual member states form the first line of defense. Cho suggests that national governments should establish mandatory cybersecurity requirements for critical infrastructure—ensuring owners and operators comply with these requirements—and provide security advice as needed. He also advocates for establishing an institutional cooperation mechanism (such as a public-private critical infrastructure security council and a joint cyber response team) so that CI stakeholders’ unique capabilities can be integrated at the national level.

Malcolm Baker provides the final chapter in the “tools to build CISR” section and fittingly it focuses on “Crisis Management and Response.” Crisis management is an essential component of the Alliance’s Strengthened Resilience Commitment announced in June 2021 as part of the NATO 2030 initiative. Baker, however, asks whether the Alliance’s current philosophy of crisis management is keeping up with mainstream developments in contemporary crisis management and thought leadership. Further, within the construct of CISR efforts, is NATO’s crisis management approach still fit for its purpose—or could it be improved? For NATO, understanding crisis management exclusively in terms of armed conflict and other hostilities may no longer be appropriate or optimal, he suggests (especially in light of the various physical, cyber, and hybrid threats earlier outlined in chapters 2–4). Baker recommends that effective CISR measures can be improved by developing and implementing robust crisis management structures and processes. The key elements of effective crisis management are early warning, an effective strategy, good communication, leadership, and swift decision making. Baker offers a proven crisis-management framework, based on the British Standards Institution, using a staged approach of: anticipate and assess, prepare, response and recovery. Finally, he reviews new developments in resilience and crisis management and offers suggestions for how NATO could better align its activities to support NATO 2030.