Countering Terrorism on Tomorrow’s Battlefield:
Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)
Sarah J. Lohmann
Editor
Lucas M. Cox, Denise Feldner, Trevor P. Helmy, Frank J. Kuzminski, Sarah J. Lohmann, Marcus Mohlin, Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu, Silke Ruhl, Sabrina Schulz, Máté Tóth, Megan A. Ward
Contributors

What do election infrastructure, space, drones, and disinformation have to do with each other? How can medical resilience be strengthened, and how are terrorists using broken supply chains, energy security, and climate change to sow chaos and destruction? Malicious actors are laying the groundwork for victory on tomorrow’s battlefield by using the same innovation and critical infrastructure democracies are using to save lives. Terrorists, however, are using new technologies to extinguish lives.

Ensuring the resilience of NATO member states is vital to the success of NATO missions and the integrity of the Alliance itself. Without resilience, the Alliance and its member states’ critical infrastructure systems are vulnerable to various threats, including terrorist attacks, hybrid attacks, and asymmetrical warfare. While technological innovation and infrastructure interdependencies heighten the risks of cascading effects, the systems providing resilience against these threats are becoming obsolete. If NATO does not create new defenses, it will be possible for a NATO adversary, whether a terrorist organization or a nation-state, to strike a single decisive blow.

Countering Terrorism on Tomorrow’s Battlefield assesses new technologies, civil-military cooperation, interoperability, and a whole-of-government approach as ways to strengthen NATO’s resilience. It also examines where innovation needs to be hardened to ensure Alliance security. The same big-data analytics the US military has used to hunt terrorists are being used by the Taliban to target innocents. Space systems provide critical capabilities to enable NATO’s core missions of deterrence and defense, including secure communications (SATCOM), positioning, navigation, and timing (PNT), early warning, environmental assessment, and intelligence, surveillance, and reconnaissance (ISR). However, the proliferation of counter-space technologies renders these systems vulnerable to interference and attack by state and non-state actors. Terrorists and adversaries with lower defense budgets and less training are making gains on battlefields due to drones, even as NATO is increasing its counter-unmanned aerial vehicle (UAV) capacities.
The story does not end there. NATO member states are working together to strengthen UAV prowess through joint exercises. Disinformation and hacked election infrastructure are being countered through targeted information campaigns and updated cybersecurity protections. Medical resilience is being strengthened through new pandemic tracking and early-warning systems. Energy security requires a unified political, economic, and military approach of member states that will bring long-term energy independence. In addition, NATO is creating healthier supply chains within the Alliance rather than turning to unreliable outside partners. The impacts of climate change on military preparedness are forcing new methods of preparedness and equipment.

This second handbook on critical infrastructure security and resilience for NATO’s Centre of Excellence in the Defence Against Terrorism analyzes today’s emerging threats, their trajectory, and how equipped NATO is to handle them. It provides recommendations and suggests new tools for foresight, preparedness, and response to these threats. We hope this research serves as a foundation to strengthen Alliance defenses today—and for decades to come.