SSI STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH~WISDOM

NATO CYBERSPACE CAPABILITY: A STRATEGIC AND OPERATIONAL EVOLUTION

Jeffrey Caton

The founding principles of North Atlantic Treaty Organization (NATO) were the collective defense, crisis management, and cooperative security amongst its member countries. Conceived in a Cold War environment, the Alliance has endured strategic changes through major conflicts and global power shifts that eventually led to the fall of the Warsaw Pact. After a brief period where some pundits questioned its relevancy, NATO has experienced a renaissance of its core security functions with the adoption of a new Strategic Concept in 2010.

The development of cyberspace defense capabilities for NATO has been making steady progress since its formal introduction at the North Atlantic Council Prague Summit in 2002. Bolstered by numerous cyber attacks such as those in Estonia in 2007, Alliance priorities were formalized in subsequent NATO cyber defense policies that were adopted in 2008, 2011, and 2014.

This monograph examines the past and current state of NATO's cyberspace defense efforts by assessing the appropriateness and sufficiency of them to address anticipated threats to member countries, including the United States. This analysis focuses on the recent history of NATO's cyberspace defense efforts and how changes in NATO's strategy and policy writ large embrace the emerging nature of cyberspace for military forces, as well as other elements of power.

In general, the topics presented are well documented in many sources. Thus, this monograph serves as a primer for current and future operations and provides senior policymakers, decision-makers, military leaders, and their respective staffs with an overall appreciation of existing capabilities as well as the challenges, opportunities, and risks associated with cyberspace-related operations in the NATO context. The scope of this discussion is limited to unclassified and open source information; any classified discussion must occur within other venues.

This monograph has three main sections:

- NATO Cyberspace Capability: Strategy and Policy. This section examines the evolution of the strategic foundations of NATO cyber activities, policies, and governance as they evolved over the past 13 years. It analyzes the content of the summit meetings of the NATO North Atlantic Council for material related to cyber defense. It also summarizes the evolution of NATO formal cyber defense policy and governance since 2002.
- NATO Cyberspace Capability: Military Focus. NATO cyber defense mission areas include NATO network protection, shared situational awareness in cyberspace, critical infrastructure protection, counter-terrorism, support to member country cyber capability development, and response to crises related to cyberspace. This section explores these mission areas by examining the operations and planning, doctrine and methods, and training and exercises related to NATO military cyberspace activities.

- Key Issues for Current Policy. The new Enhanced Cyber Defence Policy affirms the role that NATO cyber defense contributes to the mission of collective defense and embraces the notion that a cyber attack may lead to the invocation of Article 5 actions for the Alliance. Against this backdrop, this section examines the related issues of offensive cyberspace, deterrence in and through cyberspace, legal considerations, and cooperation with the European Union.

This monograph concludes with a summary of the main findings from the discussion of NATO cyberspace capabilities and a brief examination of the implications for Department of Defense and Army forces in Europe. Topics include the roles and evolution of doctrine, deterrence, training, and exercise programs, cooperation with industry, and legal standards.

NATO cyberspace activities face many challenges that must be assessed and prioritized on a recurring basis by policymakers. This monograph posits that the overall state of cyberspace activities within NATO appears to be sound and that the continued resourcing for, and pursuit of, improved cyberspace capabilities by U.S. military forces in Europe will help to ensure the steady progress of NATO cyberspace endeavors.

*****

This Publication

SSI Website

USAWC Website