REINVIGORATING STRATEGIC THOUGHT WITHIN NATO TO AVOIDING SOFT SPOTS IN NATO'S CYBER ARMOR

Dr. Panayotis A. Yannakogeoros
(Cyber defense analyst at the Air Force Research Institute)

Note: **The views expressed are his own and do not necessarily reflect those of the Air University or U.S. Air Force.**

Throughout its history, airpower has remained a cornerstone of the NATO Alliance and will remain so well into the future. The geostrategic environment NATO will face in the 21st century is certain to bring new threats and opportunities that diverge significantly from those it faced in the 20th century. What is needed is a common framework within which partners can tackle emerging threats. One such area is in responding to cyber threats. In order to be ready for any future, Airmen across the Alliance must adapt their understanding of cyberpower to conform to the needs of the evolving technological trends and their influence on the global security environment to ensure that our Alliance and our individual nations continue to enjoy the benefits of freedom and security. Doing this in a time of constrained resources and gaps in political will be challenging.

Reinvigorating strategic thought within NATO air forces requires all Alliance members to develop an understanding of the critical capabilities the Alliance will require to invest in so that the Alliance may conduct unified actions. Such challenges will require innovative thinking, especially in the uses of cyber power, if the Alliance is to maintain global and regional influence during a time of constrained defense budgets. Continued success will likely come as we integrate cyber with traditional air capabilities. Transatlantic partners have a unique role to play by bringing their robust cyber body of knowledge, to assist the United States in forging a common framework recognizing cyberspace operations as a critical specialty for Airmen with promotion potential and dedicated funding. Airmen must pursue a more aggressive approach to developing and lobbying for cyber as a capability—understanding that the ability to fly, fight, and win depends on seamlessly integrating cyber with air and space power. Cyber superiority will ensure the reliability of data used for decision making in all domains, and allow for kinetic effects via exploitation of cyber vulnerabilities. However, it is not enough for a fraction of Alliance members to possess the skill sets and invest in cyber programs. It's a capability that will need to be developed by all Transatlantic partners.

Differences within NATO as to what threats in the 21st century are plenty. Cyber conflict is clear and present that requires a common understanding to guide Alliance actions in the domain. Future conflicts may look more like the recent Russo-Georgian conflict, in which a cyber offensive preceded a conventional attack.[1] Cyber-weapons will increasingly target critical infrastructure, as Stuxnet did.[2] Conflicts will thus be more specifically targeted in terms of time and space, and the first salvos of a conflict may not be detected until the second- and third-order

[1] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook" *Parameters* (Winter 2008) http://www.carlisle.army.mil/USAWC/PARAMETERS/Articles/08winter/korns.pdf
[2] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier* http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf

effects of initial strikes manifest themselves. This is particularly true of any conflict that pits NATO against Russia, whose cyber capabilities are among the best in the world. Rather than relying solely on traditional integrated air defenses, adversaries will compete for control of the air using integrated denial strategies exploiting vulnerabilities in the cyber domain. As airpower leaders and their forces are currently heavily reliant on cyber assets, changes need to be made in how the Alliance cooperates in the cyber domain not only in the operational sense, but in the strategic sense as well. As Airmen move toward the future, the force structure—and, consequently, force-development programs—must change to emphasize the integration cyber power-projection capabilities. In other words, when formulating options to defend the nation's interests, Airmen should present proposals that fully integrate cyber capabilities into the solution.

The global nature of cyberspace makes Alliance cooperation even more important than in the other domains given the global extent and near-light speed with which cyber disruption occur. Estonia was rescued from malicious cyber actors disrupting digital services via ad hoc support. While not crossing the threshold of cyber war, these attacks highlighted that the Alliance did not have strategy or doctrines of response to specific acts against partner's sovereign cyberspace. NATO's establishment of the Cooperative Cyber Defense Center of Excellence (CCDoE) "provides NATO a wide range of products and services in the domain of cooperative cyber defense, it is not an operational centre, and does not fall within the NATO command structure."[3] Its mission is to "enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation."[4] This is the sort of concerted effort

[3] NATO Cooperative Cyber Defense Centre of Excellence. Institutional Status: http://www.ccdcoe.org/38.html
[4] Ibid. "Mission and Vision" http://www.ccdcoe.org/11.html

that will allow NATO to reach a consensus on threats and responses, formalize strategy and maintain a doctrinal edge by fusing knowledge to develop a formidable cyber force. America's recent sponsorship of the institution, after its need for it was articulated by norm entrepreneurs and then institutionalized, will assure its success.[5]

NATO Air forces must begin the process of fusing air, space, and cyber capabilities into existing and future platforms and systems. For example, aircraft currently rely on the global positioning system (GPS)—a hybrid cyber and space asset—and a range of information technology systems, but much more is possible at the individual platform level and in support of command and control.[6] Integrating offensive and defensive capabilities across the three domains will prove a key enabler and force multiplier over the coming decades. This suggests the need for systems, operators, and organizations that are capable of achieving effects in more than one domain. It also requires NATO work more closely in developing systems that are interoperable. Offensive and defensive cyber capabilities must be fused into air and space platforms. Developing such systems and conducting cooperative cyber operations, in order to obtain more refined Alliance cyber capabilities will enhance NATOs posture.

Conclusion

In the near future, cyber capabilities may become the greatest power-projection tools in NATO's arsenal, serving as both force multipliers and an Achilles' heel. Several nations already have fielded impressive capabilities for launching cyber attacks and exploiting vulnerabilities within

[5] For further discussion of the importance of American sponsorship of policy initiatives aiming to influence the behavior of states, and the process through which it is most likely to succeed, see Simon Reich Global Norms, American Sponsorship and the Emerging Pattern of Global Politics (Palgrave 2011). Also, see Panayotis A. Yannakogeorgos, "Cyberspace: The New Frontier and the Same Old Multilateralism" in Simon Reich Global Norms, American Sponsorship and the Emerging Pattern of Global Politic (Palgrave 2011).

[6] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London, UK: Frank Cass 2004).

commercial and critical infrastructure control systems.[7] Despite on-going attempts to organize, train, and equip to meet cyber requirements, Airmen across the Alliance must recognize that ability to conduct robust cyber operations is essential to both the current and future operation of non-cyber elements of the force.

[7] Brian Grow, Keith Epstein, and Chi-Chu Tschang, "The New E-Spionage Threat: A Business Week probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps." In Business Week (April 21, 2008).
Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," Washington Post January 19, 2008; Page A04.
Timothy L. Thomas, "Russian View on Information Based Warfare" Originally Appeared in Airpower Journal Vol. X, EE, Special Edition 1996 25-35, 26.