NATO and Cyber Defense: Hanging Together or Hanging Separately?

John B. Sheldon, Ph.D.
School of Advanced Air & Space Studies, Maxwell AFB, Alabama, USA
Disclaimer

The views expressed by me in this forum are mine alone and do not, in any way, represent the views of the School of Advanced Air & Space Studies, the U.S. Air Force, Department of Defense, or any other agency or department of the United States Government.
Overview

• NATO on Cyber Threats
• NATO Cyber Initiatives
• Proposed NATO Cyber Red Team
• Cyber Red Team Challenges
• Why NATO Will Not Go On the Cyber Offensive
• Wider International Implications
• Questions?
NATO and Cyber Power

“We must all hang together, or assuredly we shall all hang separately.”

Benjamin Franklin
NATO on Cyber Threats

• Official commitments to tackle cyber threats have been made, with increasing granularity, at the Prague (2002), Riga (2006), Bucharest (2008), Strasbourg/Kehl (2009), and Lisbon (2010) NATO Summits.

• Lisbon NATO Summit (2010) adopted new Strategic Concept, *Active Engagement, Modern Defence*; cyber issues are prominent throughout.

• Strategic Concept commits NATO to: “develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;”
NATO and Cyber Initiatives

• 2002 Prague Summit establishes NATO Computer Incident Response Capability (NCIRC).

• Initiative in response to DDoS attacks against NATO websites by pro-Serbian hackers during 1999 Kosovo conflict.

• NCIRC role to detect and prevent attacks against NATO systems; provide policy & forensic support to member states
NATO and Cyber Initiatives

• In response to 2007 Estonian cyber attacks, NATO defense ministers called for cyber defense framework (summer 2007).

• NATO Cyber Defense Policy approved January 2008.

• Policy creates Cooperative Cyber Defense Center of Excellence (CCDCoE), Tallinn, Estonia; and Cyber Defense Management Authority (CDMA) – both fully operational.
NATO and Cyber Initiatives


• New policy aims to bring NCIRC up to full strength by 2012; integrate cyber threats into NATO defense planning process; emphasis on prevention and resilience; creates framework for NATO assistance to member states – to include rapid reaction teams (RRT’s).
Cyber Red Team?

- 2011 NATO Cyber Defense Policy “sets out the framework for how NATO will assist Allies, upon request, in their own cyber defence efforts, with the aim to optimise information sharing and situational awareness, collaboration and secure interoperability based on NATO agreed standards.”

- So-called ‘Cyber Red Team’ is a proposal to fulfill the requirements set out by the framework.
Cyber Red Team

Purpose of proposed Cyber Red Team (CRT) would be as follows:

• Assess overall effectiveness of security measures and processes in providing NATO mission assurance;

• Demonstrate mission-level impact of cyber attacks; and

• Improve ability of NATO cyber equities to cope with emerging cyber threat environment.
Cyber Red Team

• CRT mission would simulate cyber attacks, at request of NATO clients, as a “comprehensive attempt at finding all vulnerabilities in a system.”

• CRT would demonstrate to senior decision makers political and mission implications of cyber attacks, not focus on technicalities.

• Intention is to improve NATO defenses and resiliency, not create nascent NATO offensive cyber capability.
Cyber Red Team Challenges

Proposed CRT faces several challenges:

• Legal – each NATO member state has legal autonomy regarding use of cyber capabilities; also, privacy laws impact role of CRT in member states.

• Collateral damage – simulated cyber attacks can lead to unforeseen consequences and reactions.

• Perception – is NATO developing an offensive cyber capability?
Challenges to NATO

- Cyber attacks respect no international boundary, institutional purview, or organizational stovepipe. Can threaten alliance cohesion.

- Wide disparities among NATO members in legal, policy, and doctrinal views on cyberpower.

- Inability to ‘hang together’ due to these challenges, could mean ‘assuredly hanging separately’ in event of major cyber attack against NATO, or one of its member states.
Why NATO Will Not Go on the Cyber Offensive

• Coordinating cyber defense NATO standards, procedures, policies and doctrine across 28 member states challenging enough.
• No agreement within NATO on invocation of Article 5, or when a cyber attack might trigger conflict.
• Individual member states may have offensive cyber capability not for NATO use; such capabilities too sensitive and perishable to share with even close allies.
• Wider malaise about overall purpose of NATO among some member states.
Wider International Implications

• Wider (beyond NATO) cyber defense initiatives face even greater challenges.
• Given rapid offense-defense cycles in cyber, states, even close allies, unlikely to share offensive cyber capabilities, or easily give them up.
• Efforts at creating cyber ‘rules of the road’ or international norms, while worthwhile in principle, will likely be contentious, incremental at best, and will not prevent use of offensive cyber capabilities.
• Unique characteristics of cyberpower render traditional instruments lacking or irrelevant.
Questions?