BEST DEFENSE

NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons

Not many people noticed it, but last month, NATO made a dramatic change in its cyber policy.

BY THOMAS E. RICKS | DECEMBER 7, 2017, 10:15 AM

By Col. Rizwan Ali, USAF (Ret.)
Best Defense office of cyber deterrence

Not many people noticed it, but last month, NATO made a dramatic change in its cyber policy announced by the NATO Secretary General that arguably was the alliance's biggest overall policy shift in decades. Having led the policy discussions in several NATO committees for the past four years on the use of cyber capabilities and cyber weapons, I can tell you this was the most hotly debated and contentious decision during my tenure at NATO.

In short, NATO embraced the use of cyber weaponry in NATO operations. This is a marked departure from NATO's historical stance of using cyber only defensively, mainly to ward off incursions against its own networks. The more aggressive approach was intended as a strong message, primarily to Russia, that NATO intends to use the cyber capabilities of its members to deter attacks in the same way it uses land, sea, and air weaponry.

Russia's provocative actions during the U.S. Presidential elections, its attempts to influence the French and German elections, and its blatantly aggressive, and on-going cyberwar against Ukraine were likely key determining factors which led the NATO defense ministers to adopt a more assertive stance.

On the surface, NATO's cyber policy shifts might seem to be little more than incremental changes to its existing policy. However, the fact the alliance is standing up a cyber operations center to integrate cyber capabilities from alliance members sends a message

to the world, especially Russia, that alliance members both possess and have the will to use their cyber capabilities and weaponry during military operations.

This is not the first time NATO has tried to assert itself in cyberspace. In 2008, NATO's first cyber defense policy was adopted and NATO's Cooperative Cyber Defense Center of Excellence in Estonia was established, following the devastating cyberattacks on Estonia by Russia. Unfortunately, this policy was purely about the defense of NATO's own networks. Plus, the establishment of the center in Estonia did little to dissuade Russia's aggressive actions in cyberspace.

Implementing this new cyber policy will be an uphill battle for NATO. In an interesting wrinkle, the cyber effects (a.k.a. cyber weaponry) will be provided by the alliance members and will be fully controlled by the ally which provided the specific capability. This is a striking departure from the way NATO handles the command and control of other capabilities and forces provided by its members. If a member nation provides a squadron of airplanes, those airplanes and its crew come under the full operational control of the assigned NATO military commander. In the case of cyber, the nation providing the cyber capabilities will retain all command and control of its cyber weaponry and cyber forces. None of these will be brought under the traditional operational control of the NATO commander.

This 'black box' approach to military operations is one which military leaders rarely employ, because it is fraught with problems. When executing operations, military commanders want to know the details about the capabilities available to them, to include the limitations. They also want to know the potential conflicts that capability may present with other ongoing operations and the legal implications on the use of that capability. In the path laid forward by the defense ministers, these details may not be available to the NATO commanders. The commanders will request an effect using cyber weaponry during an operation and one of the allies will provide that effect without any further information. This is far from ideal but something NATO's military commanders will have to solve through revamped procedures.

In addition to the opaque nature of NATO's employment of cyber weapons, NATO's commanders will have to overcome two additional challenges. First, they will have to find a way to share more intelligence with each other for the cyber domain. Nations control cyber intelligence more tightly than most other type of intelligence. This is because of the highly clandestine nature of how the intelligence was obtained. Such intelligence is not even shared internally within the nation's government, let alone with allies.

Second, a cyber weapon is fundamentally different than a traditional weapon. The fact that an adversary knows about a traditional weapon, such as an F-22, does not negate its effect and the F-22 can be used many times against the same adversary. However, with

cyber weapons, once that weapon is used, the adversary knows about the cyber techniques employed and an adversary can readily build cyber defenses to prevent future attacks using that cyber weapon. Essentially, cyber weapons are one-use weapons. This makes it likely that Allies will be reluctant to share and use their cyber weapons with NATO unless their own national survival is at stake.

Despite these challenges, NATO's adoption of this significantly more aggressive cyber policy, one which allows the use of cyber weapons in operations, is a big step forward to establishing a credible deterrence capability for NATO in cyberspace. Several alliance members have openly declared they possess cyber weapons. The fact that these allies agreed to make their sophisticated cyber weaponry available for use during NATO operations should give potential adversaries considerable pause.

Col. *Rizwan Ali, USAF (Ret.) led the team that wrote and implemented NATO's new cyber policy and NATO's military cyber strategy. He is a cybersecurity policy fellow at New America and the author of Cyber: NATO's Newest Domain.*

Thomas E. Ricks covered the U.S. military from 1991 to 2008 for the Wall Street Journal and then the Washington Post. He can be reached at ricksblogcomment@gmail.com.

TAGS: BEST DEFENSE, CYBER, CYBERATTACKS, ESTONIA, EUROPE, MILITARY, NATO, RUSSIA, VOICE

SHOW COMMENTS