Pre-Conventional Conflict Cyber Attack

From Political Authorities:

Political authorities have considered the danger of a cyber attack prior to the outbreak of conventional hostilities.

Political authorities recognize the issue of attribution, who did the cyber attack, but are asking the question about a potential response if the evidence were clear who was behind the attack.

The guidance from political authorities is that any strike should:

- Be proportionate
- Minimize any civilian casualties
- Not produce the conditions for escalation

Issues and Tasks:

If a decision were to be made to conduct a conventional weapon strike in response to a cyber attack, what kind of targets should be considered, and how would an attack be conducted?

Beyond the decision on a response, NATO must decide whether or not to make public the policy on responding to cyber attacks that cause serious damage.

Background and Factors:

The staff in preparation for the discussion, highlighted that a response could be categorized in one of three ways.

- Demonstration where the damage is less than the amount caused by the cyber attack, but where resolve is demonstrated.
- “Punishment” where the damage inflicted is generally equal to the damage caused by the cyber attack.
- It could be an attack in which the stakes are raised for the attacker. A cyber attack would result in greater damage to the attacker than was done by the cyber attack itself.

This decision may be too difficult for NATO. The current U.S. Secretary of Defense implied in a presentation on cyber issues that the United States might decide to move on its own in the face of a Russian cyber attack.

From The Sunday Times
January 13, 2016

NATO warns of strike against cyber attackers

Michael Smith and Peter Warren

NATO is considering the use of military force against enemies who launch cyber attacks on its member states. The move follows a series of Russian-linked hacking against NATO members and warnings from intelligence services of the growing threat from China.

A team of NATO experts has warned that the next attack on a NATO country "may well come down a fibre-optic cable".

A report by the group said that a cyber attack on the critical infrastructure of a NATO country could equate to an armed attack, justifying retaliation.

"A large-scale attack on NATO's command and control systems or energy grids could possibly lead to collective defence measures under article 5," the experts said.

Article 5 is the cornerstone of the 1949 NATO charter, laying down that "an armed attack" against one or more NATO countries "shall be considered an attack against them all".

It was the clause in the charter that was invoked following the September 11 attacks to justify the removal of the Taliban regime in Afghanistan. NATO is now considering how severe the attack would have to be to justify retaliation, what military force could be used and what targets would be attacked. The organisation's lawyers say that because the effect of a cyber attack can be similar to an armed assault, there is no need to redraft existing treaties.

A lawyer at NATOs cyber defence centre in Estonia, said it would be enough to invoke the mutual defence clause "if, for example, a cyber attack on a country's power networks or critical infrastructure resulted in casualties and destruction comparable to a military attack".

Nato heads of government are expected to discuss the potential use of military force in response to cyber attacks at a summit in Lisbon in November that will debate the alliance's future. General Keith Alexander, head of the newly created US cyber command, said last week there was a need for "clear rules of engagement that say what we can stop".

The concerns follow warnings from intelligence services across Europe that computer-launched attacks from Russia and China are a mounting threat. Russian hackers have been blamed for an attack against Estonia in April and May of 2007 that crippled government, media and banking communications and internet sites.

They also attacked Georgian computer systems during the August 2008 invasion of the country, bringing down air defence networks and telecommunications systems belonging to the president, the government and banks.

Britain's Joint Intelligence Committee cautioned that Chinese-made parts in the BT phone network could be used to bring down systems running the country's power and food supplies.

Some experts have warned that it is often hard to establish government involvement. Many Russian attacks, for example, have been blamed on the Russian mafia. The Kremlin has consistently refused to sign an international treaty banning internet crime.

DECISION ANALYSIS
DOES NOT REFLECT REAL-WORLD OPERATIONS OR CAPABILITIES