Redefining Article Five?

Maxim Worcester

November 2014

Abstract

Following the announcement at the NATO summit in Wales that cyber defense is a part of NATO's core task of collective defense and the UK's statement in 2013 that it was developing cyber-attack capability it has become clear, that the time has come to rethink the definition of Article Five of the NATO Charter.

This step becomes yet more relevant when seen in the light of Russia's hybrid attacks and illegal occupation of the Crimea and parts of eastern Ukraine.

The author argues that a redefinition of Article Five to include all forms of hybrid warfare only makes sense when NATO is in a position to respond by using the same methods as the attacker. In order to do so, NATO needs to develop a centralized and comprehensive hybrid attack capability, including the ability to conduct offensive cyber warfare.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented, and impartial to party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, that bring major opportunities but also risks, decision makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics relating to politics, economy, international relations, and security/defence. ISPSW network experts have operated in executive positions, in some cases for decades, and command wide-ranging experience in their respective areas of specialization.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

NATO leaders agreed at the Wales Summit in the autumn of 2014 that a large-scale cyber-attack on a member country could be considered an attack on the entire U.S.-led alliance, potentially triggering a military response. As former NATO Secretary-General Anders Fogh Rasmussen said "Today we declare that cyber defense is part of NATO's core task of collective defense".

Calls to include non-traditional or hybrid attacks as a reason for invoking Article Five are not new. In a speech to the Atlantic Council in early 2010 former Secretary of State Hilary Clinton strongly suggested that attacks on allied cyber and energy infrastructures should be reconsidered attacks under Article Five of the NATO Charter. Her predecessor, Madeleine Albright, concluded in 2010 that "the next significant attack on the Alliance may well come down a fibre optic cable".

The statement made by the former NATO Secretary-General clearly leaves room for maneuver. If NATO were, for example, to strike the word "armed" from the definition of Article Five and furthermore clearly define what is meant by an attack on NATO, it could place the members in a bind. A cyber-attack might then technically meet the definition put forth in advance without the actual circumstances generating consensus for action. A situation could also arise as the risks of retaliation might simply outweigh the damage done by the aggressor. Members might be put into the awkward position of having to choose between the credibility of NATO and their own short-term interests.

There is a value in strategic ambiguity. In the cyber case drawing a line in the sand virtually invites actions just short of casus belli. By simply declaring that there may be circumstances in which NATO will consider a cyber-attack on one of its members an attack on all is a greater deterrence. Given the general reluctance of the voting population in Europe to get involved in any form of kinetic exchange, such ambiguity would also give politicians the degree of freedom they need to retain the confidence of their public.

The current debate on defining what action might be considered an attack under Article Five is, however, more far-reaching than simply a cyber-attack. Besides such attacks we also need to consider sophisticated information operations, psychological attacks, economic warfare, social engineering and proxy attacks.

In part due to the relative weakness of its conventional military capabilities, Russia has focused on such hybrid tactics which are more difficult for NATO to counter and can be employed alongside conventional means of warfare. As the Russian Chief of General Staff, Valery Gerasimov, put it in February 2013: "The very rules of war have changed. The role of nonmilitary means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of weapons in their effectiveness". In his speech he goes on to say that in the 21st century we have seen a tendency towards blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template. Gerasimov furthermore emphasizes the importance of coordinating the use of traditional warfare with hybrid tactics. Such a strategy has become possible through the advances in command and control systems making military actions more dynamic, active and fruitful.

In the run up to the occupation of Crimea and the eastern part of the Ukraine Russia employed the full gamut of hybrid tactics. Russia and Ukraine traded cyber-attacks during the referendum on Crimea. Reports indicate that NATO and Ukrainian sites suffered DDoS (denial of service) attacks during the vote. As in the case of Russia's earlier confrontations with Estonia and Georgia, the attacks seemed to have come from mercenaries

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

or state backed "patriotic hackers" rather than from the armed forces or intelligence agencies. In other words the job was handed off to proxies thus giving Russia plausible deniability.

The dissemination of false information, known as concentrated information operations (INFOOPS) was and is being used by Russia in the Ukrainian conflict. Russian media keep repeating that the regime change in Kiew was a "fascist plot" and a repeat of the 1941 German invasion of the Soviet Union. Such disinformation, especially in the eastern part of the country, led to a strong support in the population for the separatist movement. Such information operations have also encouraged the population to undertake subversive activities against the Ukrainian state. INFOOPS is in essence a form of social engineering and Russia is using social engineering to both influence public opinion in the Ukraine and in Western Europe. Such a tactic has resulted in dividing the population in the Ukraine and has had a significant impact on public opinion in the West to the extent that some politicians have argued to accept the status quo with regard to Crimea. Such moves are very much a part of hybrid warfare and serve to weaken the resolve of the enemy.

Beyond INFOOPS lies the third, most alarming level of cyber conflict: attacks on critical infrastructure, public and private, with the aim of disrupting or disabling essential services. Targets could include the banking sector, energy grids, road signals and certainly military communication networks. If the Ukraine conflict escalates to this level it means the formal onset of cyber war. This would make the onset of a kinetic conflict more than likely.

Besides the current cyber conflict we are also witnessing an increased level of proxy attacks by a combination of regular and irregular combatants. In the case of the Crimean occupation it has since become clear that the "little green men" were Russian Special Forces troops declared as volunteers, much as it was and is the case in the eastern part of the Ukraine. The path Russia is going down is perfecting comprehensive security in order to sow comprehensive insecurity with its adversaries.

Given the level of Russian activity with a strong focus on former member states of the Soviet Union it becomes clear that NATO and the West cannot simply carry on as if nothing has changed. We need a new strategy in the West which reflects the rise of hybrid attacks and threats.

Besides measures which illustrate strategic intent, (prepositioning arms east of the German border, increasing the scale and frequency of exercises, relocation of armed forces, an increase in defense spending), NATO needs to consider taking steps to build an offensive and centralized cyber-attack capability. When the UK announced in late 2013 that it is developing the capability to carry out offensive cyber-attacks against other nations the reaction was mixed. Defense experts warned that Britain risks losing the moral high ground by this announcement and that such a step would simply give the Chinese and Russians more ammunition. Others fear that this move could turn out to be counter-productive as other actors will simply want to react in kind.

The British announcement is based on the analysis that it is no longer sufficient just to build defenses against cyber-attacks and that an offensive capability is needed to strike back against enemies and put cyber alongside land, sea, air and space as a mainstream military activity. As Carl von Clausewitz aptly observed: "A defender must always seek to change over to the attack as soon as he has gained the benefit of the defense". Such a move towards developing an offensive cyber capability also makes sense when reconsidering Article Five. If NATO is currently subject to a cyber-attack it cannot respond in kind. It can revert to economic sanctions or in

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

a final step can respond kinetically. Such an escalation, however, is a very difficult sell to a population which widely rejects the use of arms. A cyber response to a cyber-attack is an easier sell.

It also makes a great deal of sense given that nations such as the US, Israel, Russia, China and now the UK have developed or are developing the ability to destroy or sabotage other nations internet infrastructure as part of military planning and covert operations.

Brandishing cyber-attack capabilities might also back up a deterrence strategy and dissuade another state from mischief – but it must be credible, much as Mutual Assured Destruction was credible during the Cold War. Redefining Article Five only makes sense if NATO is in a position to act – and is willing to do so.

***

Remarks: Opinions expressed in this analysis are those of the author. See also:

Worcester, Maxim: Putin's Proxy Warfare Strategy
in: International Relations and Security Network (ISN), Center for Security Studies (CSS)
August 2014, ETH Zurich
http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=182503

About the Author of this Issue

Maxim Worcester is Managing Director of German Business Protection GmbH (GBP), a Berlin based Security Consultancy. GBP is a subsidiary company of KÖTTER Security. In the past he worked, amongst others, for the Economist Intelligence Unit, Frankfurter Allgemeine Zeitung, Control Risks and KPMG.

Maxim Worcester

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de