ISBN 978-3-934401-20-4

Independent Review on European Security & Defence
Volume No 3/2009

The European
Security and Defence Union

No 3/2009

The "New NATO" after the 60th anniversary of the Washington Treaty

Jaap de Hoop Scheffer,
Secretary General of NATO, Brussels

The future of ESDP – ways to improve European Security and Defence Policy

Dr. Clemens von Goetze,
German PSC Ambassador, Brussels

Airbus strives for open competition

Dr. Thomas Enders,
CEO Airbus, Toulouse

Jaap de Hoop Scheffer,
Secretary General of
the NATO , Brussels

POLICY & POLITICS

EU-NATO

SECURITY

Dr. Thomas Enders,
CEO Airbus, Toulouse

EUROPEAN DEFENCE and ARMED FORCES

INDUSTRIES

INSTITUTIONS and ASSOCIATIONS

DEFENCE & SECURITY NEWS

Cyberwar – NATO's exposed flank

By Bert Weingarten, PAN AMP AG Board, Hamburg

The security and defence pact that is NATO (the North Atlantic-Treaty Organisation) is able to pool the military potential of all its members. NATO's defensive strategy is based on the continuous monitoring of land, sea and airspace far beyond the territory it is there to defend. In this way it can gain early warning of potentially hostile military movements and analyse the degree of threat they represent in order to react immediately and appropriately. Land, sea and air forces stand available if a military reaction is called for (including the NATO Response Force). In July 2006 Secretary General Jaap de Hoop Scheffer announced plans for expanding the Alliance's defense strategy to embrace a Europe-wide missile defence programme that also included enhanced early warning through airspace surveillance. The level of sophistication attained in continuous monitoring of land, sea and airspace makes it extremely difficult for a tank regiment, formation of warships, or even smaller combat units to close in on NATO territory unnoticed. And there is virtually no chance of moving within NATO territory without being seen.

Internet – the underestimated danger

In order to appreciate the risk that the internet poses to NATO a basic definition of the word itself would be helpful. It has often been falsely assumed that the term refers to an "INTERnational NETwork", but 'inter' is taken from the Latin for "between". In fact, the internet established links between many smaller networks using a common basic language (TCP/IP). In the early days of the internet back in the sixties, military networks in the USA were linked together under the so-called "Arapnet". Then the universities, net operators and private individuals all connected up, ultimately forming the network of all networks, today's "Internet". Thanks to the speedy interconnection of international networks, today's worldwide web facilitates global communication but it also means that virtually all military networks, wittingly, and sometimes unwittingly, contain gateways to the internet. The upshot is that almost any military network can be accessed and attacked from the internet whereas the net cannot be monitored to give advance warning of an impending attack. What's more, an attack on military networks over the internet may come from outside Alliance territory, but it may actually originate inside the networks of NATO member countries.

Cyber attack on Estonia*

Contrary to the initial suspicions of the Estonian government, the attack on Estonia's IT infrastructure in 2007 was not the first act in a cyberwar launched from the Kremlin, but a coordinated attack by a few Russian IT experts and fellow hackers. The removal of a Russian war memorial from the capital Tallin at the end of April 2007 sparked off two weeks of cyber attacks against the servers of Estonia's government, political parties, banks and media companies. These attacks isolated or shut down government and administrative IT systems. Estonia's leading bank had to suspend international payments for two days. Hospitals and power grids were also affected. And the attacks went beyond targeting banks, ministries and the government: dramatically, they also went for the numbers used to contact the country's emergency services. Estonia's Computer Emergency Response team had already run a range of simulations and IT crisis scenarios but the sheer scale of these attacks overwhelmed them, coming as they did from many different networks or subnets across the globe, for example in the US or Vietnam.

Individual attacks were carried out at different bandwidths of below 10 and up to 100 megabits per second. Most were in the 10 to 30 Mbps range. Three quarters lasted fewer than sixty minutes and only 5.5% more than ten hours. For some IT security experts, the internet attack on Estonia, a country which, even by EU standards, boasted massive internet ac-

Bert Weingarten

Bert Weingarten, CEO of PAN AMP, Hamburg. Born 1970 in Hamburg, Bert Weingarten graduated from the Max-Planck-Institute, in information and communications technology. He created the first "internet project house" in Germany and developed and managed concepts for using internet access in the public sphere. He operated the first public internet focal points in Germany, and thus had a decisive role in the enlargement of the internet in Germany. With the foundation of PAN AMP in 1998, Weingarten was responsible for the development of internet electron filters and security technologies as well as automatic internet analysis and forensic processes. Weingarten supports the security scene of Europe through Key-Notes to Ministers of the Interior, Police Presidents and Directors of State Offices of Criminal Investigation. Furthermore he is as a specialist a solicited   lecturer in the audiences of the offices of the German Federal States and the Federal Government, where he optimises the skills of internet agents. With those activities Weingarten could early contribute in an essential way to the preventive calculation of dangerous situations in Europe.

Bert Weingarten during his speech at the Police Congress 2009 in Berlin

cess, high e-government standards and many online services, constitutes a new form of retaliatory action.

The Estonian government brought in NATO and the EU and called for action, including the development of a strategy to deter future cyber attacks. The Estonian incident is being taken extremely seriously in NATO circles, and one point now at issue is whether such cases should be used to invoke collective defence on the part of Alliance member countries. Immediately after the event, IT security experts travelled to Tallin from the US Department of Homeland Security as well as the Secret Services, responsible for protecting US financial services. One priority is to identify the point of origin of the attacks as the aggressors are using new peer-to-peer techniques.

IT security of NATO's Member States

The first assessment of a NATO member state in the wake of the cyber attack on Estonia was voiced by Mike Witt, the deputy Director of US-CERT. Thanks to their greater size, sophistication and variety, US government networks would resist attack more effectively, but the Estonian example had shown just how easily a country's infrastructure could be brought to a standstill. There are already criminal communities at large today offering to carry out this type of attack anywhere in the world. Even networks perceived to be secure are beset time and time again by relatively easy-to-produce IT viruses and worms. In February 2009 NATO members were hit by the "Conficker" computer worm. After several hundred German Army computers had been contaminated, individual stations cut themselves off from the army network to prevent further spreading of this malicious software. In mid-January as "Conficker" successfully penetrated as far as the French Navy's intranet, the British MOD and other NATO partners were feverishly directing resources against this new threat.

Cyberwar – conflict in virtual space

Cyberwar is a contraction of Cyberspace War and refers to military conflict [kriegerische Auseinandersetzung] waged in and around virtual space, chiefly using instruments from the realm of information technology. So far cyberattacks have only succeeded in paralysing computerised links. Hence, cyberwar is the term used to describe military conflict waged in data networks through a combination of cyber attacks and countermeasures. It is, however, conceivable that security technology could be overcome and computer systems hijacked for nefarious purposes.

Misinformation could be convincingly generated and, say, computer-driven guidance and fire control systems induced to report friendly forces as hostile. Cyberwar might ultimately lead to unintentional attacks on friendly troops or allies.

It is therefore becoming a part of asymmetric warfare and, in certain circumstances, could be an effective counter to Network Centric Warfare e.g. if a force with inferior military resources and technology were ranged against an enemy heavily dependent on electronic communication systems. In particular, the fact that a cyberwar could be mounted against the NATO Alliance from within member countries begs the question of whether, and how, the partners could stand together in the event of a cyberwar. So far there is no rule to follow on this in the NATO treaty. Under Article V, the member states undertake to ensure their collective security by taking an attack on any one of them as an attack on all and assisting the aggrieved partner. However, Article 6 limits the obligation to assisting a partner against armed attacks in the North Atlantic area.

IT line of defence of the NATO member states

Essentially, the internet has blurred front lines, connecting almost any potential aggressor to its victim and allowing no early warning. National territories now extend into the internet and whole areas there stand virtually unprotected. Moreover, conventional military means are no defence against the attack scenarios of a cyberwar. Hence the importance and urgency for all NATO member states to introduce an active line of defence into their internet backbones and gateways so that, in the event of an attack, the IT structure and equipment of Alliance states can be actively protected without delay.

* see article Tarmo Kõuts page 35 f.