ISBN 978-3-934401-20-4

Independent Review on European Security & Defence
Volume No 5/2009

The European Security and Defence Union

Main Topic
Maritime Security

No 5/2009

The role of the European Parliament in the Common Foreign Security and Defence Policy

Gabriele Albertini MEP, Chairman, Foreign Affairs Committee, European Parliament, Brussels/Strasbourg

Nuclear Disarmament and Proliferation – a personal view on the need for realism

Michael Rühle, Deputy Head of the Policy Planning Unit in the Private Office of the NATO Secretary General, Brussels

Russia's security policy in new European structures – what is behind President Medvedev's ideas

Vladimir Chizhov, Ambassador, Permanent Representative of Russian Federation to the European Union, Brussels

Cyberwar & Cyber Defence

by Bert Weingarten, CEO PAN AMP AG, Hamburg

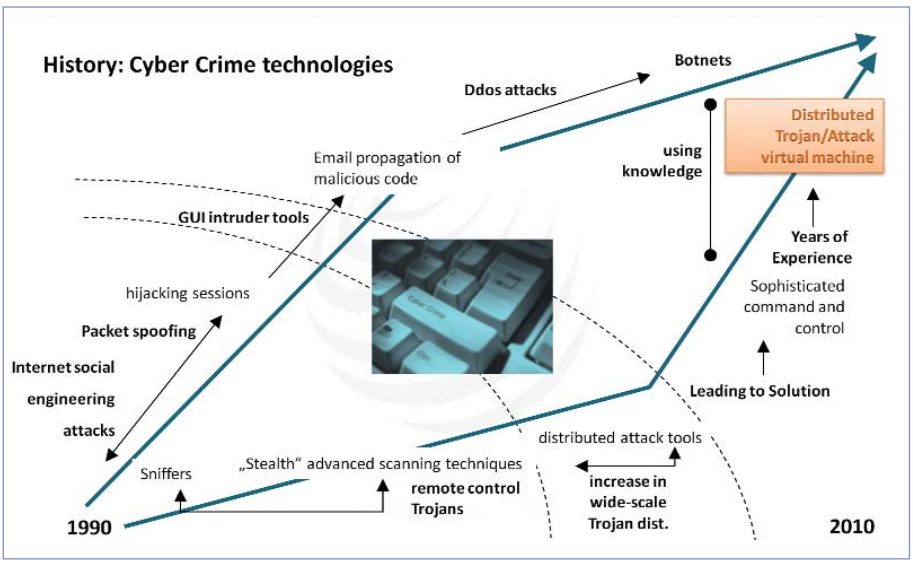
It was at the request of Dr Karl von Wogau, who presided the European Parliament's Sub-Committee on Security and Defence (2009), that I began to prepare my lecture on "Cyberwar and Defence" for the 8th Congress on European Security and Defence held in Berlin on 08 and 09 December 2009. I started by researching definitions of the term "Cyberwar" in the USA, Asia and Europe and found 840 different, and at times quite contradictory, opinions, assessments and texts. I organised print-outs of the information I had harvested into a wall display comprising three groups. The first set contained information about Cybercrime and related to the view that a cyberattack was equivalent to cyberwar. The second set reflected the opinion that individuals could conduct cyberwar, while the third mixed virtual and physical forms of attack. In fact, none of the existing assessments and opinions in any of the three sets of information was suitable. Moreover, no ranking had so far been established with regard to the seriousness of a cyberwar.

Bert Weingarten

Bert Weingarten, CEO of PAN AMP, Hamburg.
Born 1970 in Lübeck, 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 keynotes to Ministers of the Interior, Police Presidents and Directors of State Offices of Criminal Investigation. Furthermore he is as a specialist and 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 contribute early in an essential way to the preventive calculation of dangerous situations in Europe.

How to define Cyberwar?

Before defining the term "Cyberwar", it is useful to determine the things it definitely does not cover, for example cybercrime activities directed against civilian users or companies. Cybercrime technologies have multiplied since 1990 and made an evolutionary leap in 2010 with the spread of virtual systems that make it easier to participate in cybercriminal networks. Physical attacks, such as the destruction and sabotage of hardware (e.g. cables, antennas, and satellite connections) are not part of a cyberwar either, insofar as assets are physically destroyed or sabotaged e.g. through the elimination of a hardware unit, a rocket attack on a telephone exchange, or the shooting down of a communications satellite. A fair number of scientists assumed that the 1999 Kosovo conflict could be defined as the first cyberwar between nations because both sides had recourse to this type of weapon. Yet although extensive command and control of war operations using orbiting reconnaissance systems was a decisive factor on NATO's part, it cannot be seen as an element of cyber warfare, for the satellites were primarily used to gather intelligence rather than to manipulate or take over enemy weapon systems.

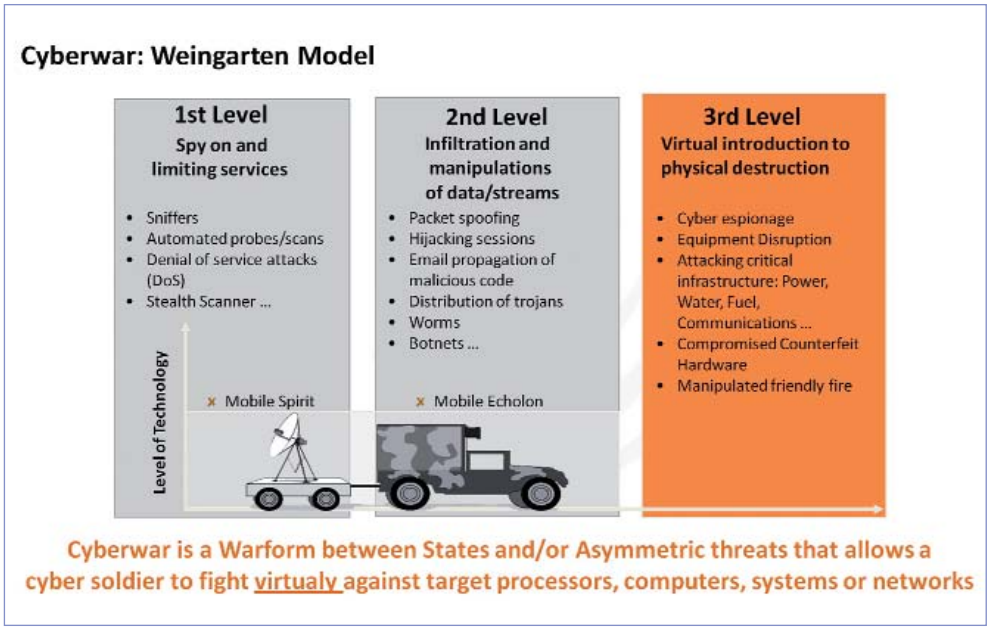


The Estonian case

Close study of analyses of the events in Estonia in 2007, and of comprehensive data on individual incidents and interpretations, for which I must thank Vice-Admiral Tarmo Kouts, MoP, (Head of the Estonian delegation to the ESDA/WEU Assembly), Tallinn, led me to conclude that they constituted an example of a successful cyberattack designed to achieve "denial of service" by targeting

government and administrative centres and preventing online access to Estonia's main bank.

In spite of the fact that hospitals, power supply systems and emergency services were also targeted in the Estonian attacks, these remain a manifestation of cybercrime. It has not been proven that any State carried out the attacks and, if a State was involved, it was only to the extent of countenancing the actions of hackers motivated by misguided patriotism.



Cyberwar is conducted between States, and/or asymmetric threats, and gives cybersoldiers the opportunity to attack processors, computers, systems or networks.

Different levels

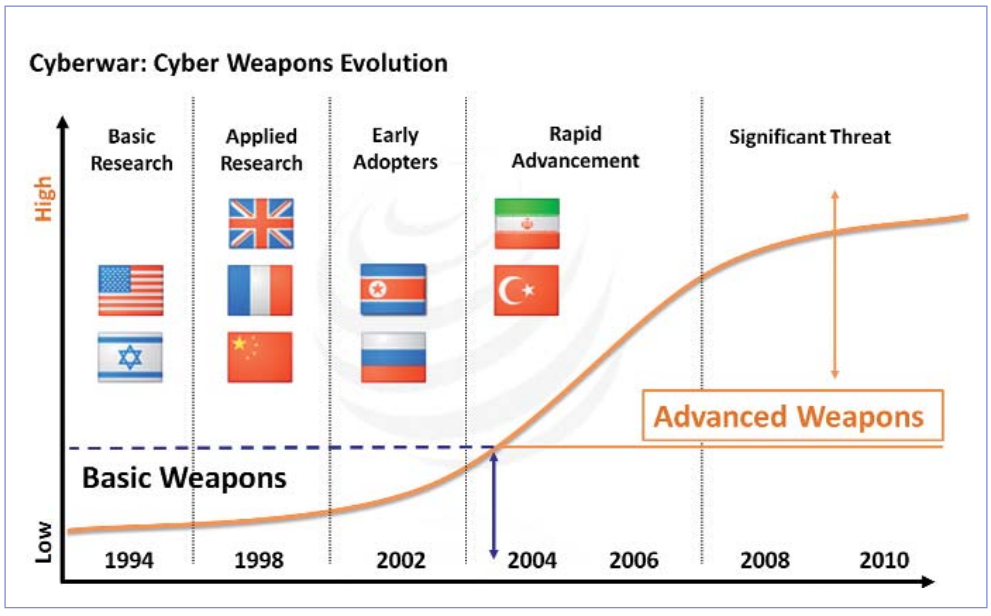
The first level in such a war is the tracing and demarcation of the resources targeted which might entail the deployment, for example, of automated sniffers, scans and denial-of-service attacks devised to suppress or disrupt enemy services.

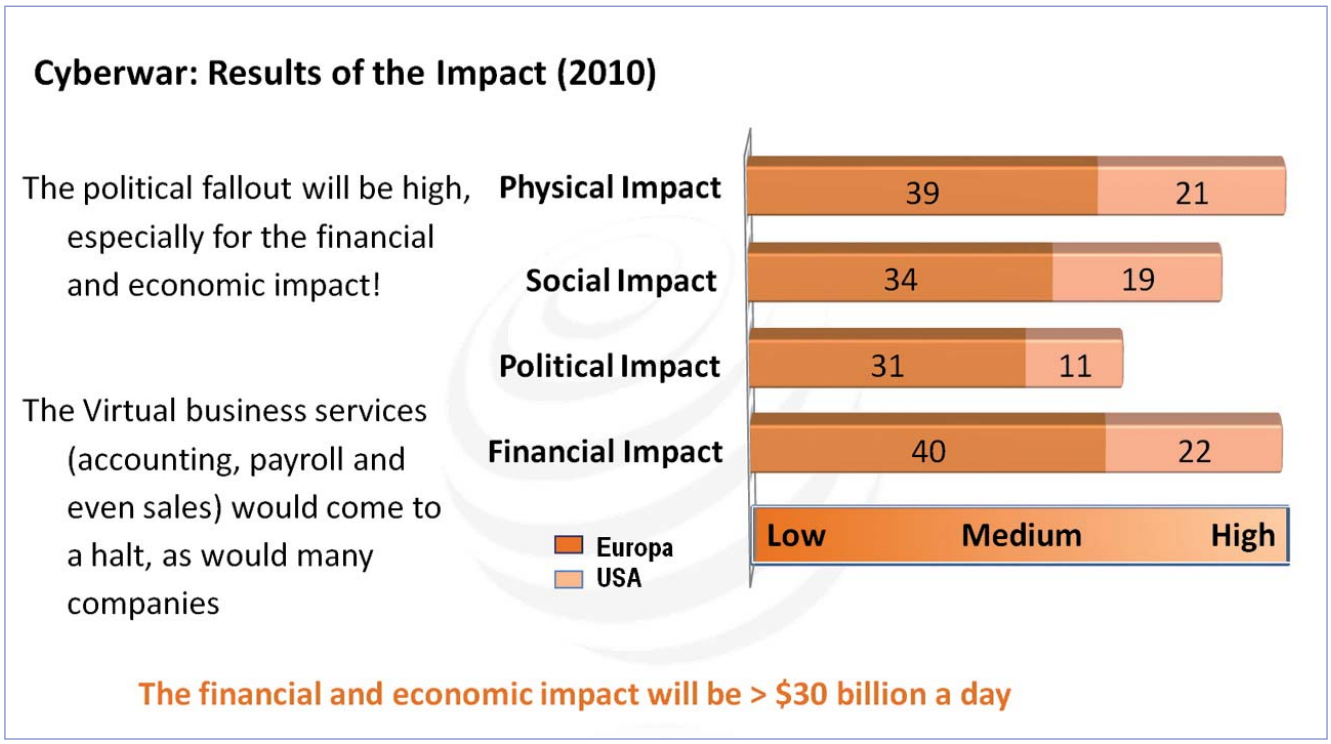
The second level is the infiltration and manipulation of data and data connections through, for example, hijacking sessions, or the use of trojans, worms and botnets to gain useful information by penetrating the adversary's computer networks. The third level involves 'virtual' manipulation to bring about the physical destruction of the resources and units targeted. Previously manipulated hard- and software can be taken over or destroyed; critical power, water and IT infrastructures may similarly be taken under control or eliminated; the remote manipulation of IFF signals can produce "friendly fire" incidents; or specific technologies and weapons may be manipulated from a distance in order to take over, or take out, enemy units.

So far – so good

The world has not experienced a cyberwar. However, a considerable number of events between 2007 and 2009 indicate that weapons have been, and are being, developed on the way to "Advanced Cyberwar Weapons". The "Information Warfare and Strategy" department in the USA began fundamental research on cyber weapons in 1994 and a number of nations have been working on digital warfare since the nineties. The successful build-up and further development of "Advanced Cyberwar Weapons" in China and the USA since 2007 could be called the beginning of the "Cold Cyberwar".

It may be assumed that 60% of all nations will have attained a basic level weapon for cyberwar operations by





2014. This makes the prospect of a future cyberwar a serious threat to Europe because in today's world, the systems needed to conduct cyberattacks can soon be obtained by States and "Asymmetric threats" alike. Estimated at between 50 000 and 100 000 euros, the low cost of developing basic weapons for online attacks means that asymmetric clashes on the web are inevitable and, indeed, already occur between Al-Qaida's terrorist conspiracy and the nations of the West.

A strong risk: the internet

There is, in particular, a strong risk that the internet will be hijacked for a cyber attack as any target system connected to the internet can be hit at lightning speed. It is estimated that there would be less than 2 seconds' warning of such an attack. In all probability, in an age when daily online access is a taken for granted, and the use of eCommerce, online-banking and social networks is a routine affair, only after an attack has occurred will we realize just how valuable the data, information and fully functioning networks are, and just how much we depend on them.

If a cyberwar were to break out, i.e. a war between nations through the internet, it would affect all the other interconnected States and wreak serious political and economic damage. An international agreement on the limitation of cyberwar weapons is needed today and should be taken up by the United Nations as a matter of urgency.

As computer systems in the USA and Europe are connected through 'backbone' networks, internet connections in the US and Europe are like a "town with over 500 gates". If all of these come under attack, they must all be defended and, in the case of a cyberwar, as more and more infrastructure is damaged, the attacks will regroup and deploy to put any intact subnet resources under strain. If a cyberwar were to be launched against the USA , it is only to be expected that European subnets would be affected. Under extreme pressure, it is possible that encrypted links such as exist on the internet between military installations, for example, might collapse.

Saudi Arabia, however, is ready to face a cyberwar. It has organised the net in a way that, to coin a military phrase, makes it a position that can be properly defended. Unlike most other countries, the Saudis can administer the internet backbone in their land directly, and partially or fully restrict capacity. The same applies for various subnets in Saudi Arabia. The government there has an effective instrument to limit damage in the event of a cyberwar and the national subnets would only be slightly affected.

Be prepared for Cyberwar

Given the possibility of a future cyberwar, it is logical and urgent to devise a European or NATO strategy for the military defence of the virtual space of the Member States. Each of the latter should, moreover, prepare for the coming cyberwar by organising an institutionalised national defence, with access to the resources needed to prepare for a war via the internet. The development of stand-alone, military infrastructures and the safeguarding of national subnets should be completed if an effective defence is to be ensured in the event of a cyberwar. Any future war will begin with an attack from Cyberspace. Only countries who have prepared for cyberwar will be able to deploy effective countermeasures.