[CYBERWAR & CYBER DEFENCE]

European Security and Defence: Bert Weingarten, CEO PAN AMP AG, Speech in extracts, 09.12.2009

Berlin, 9. December 2009

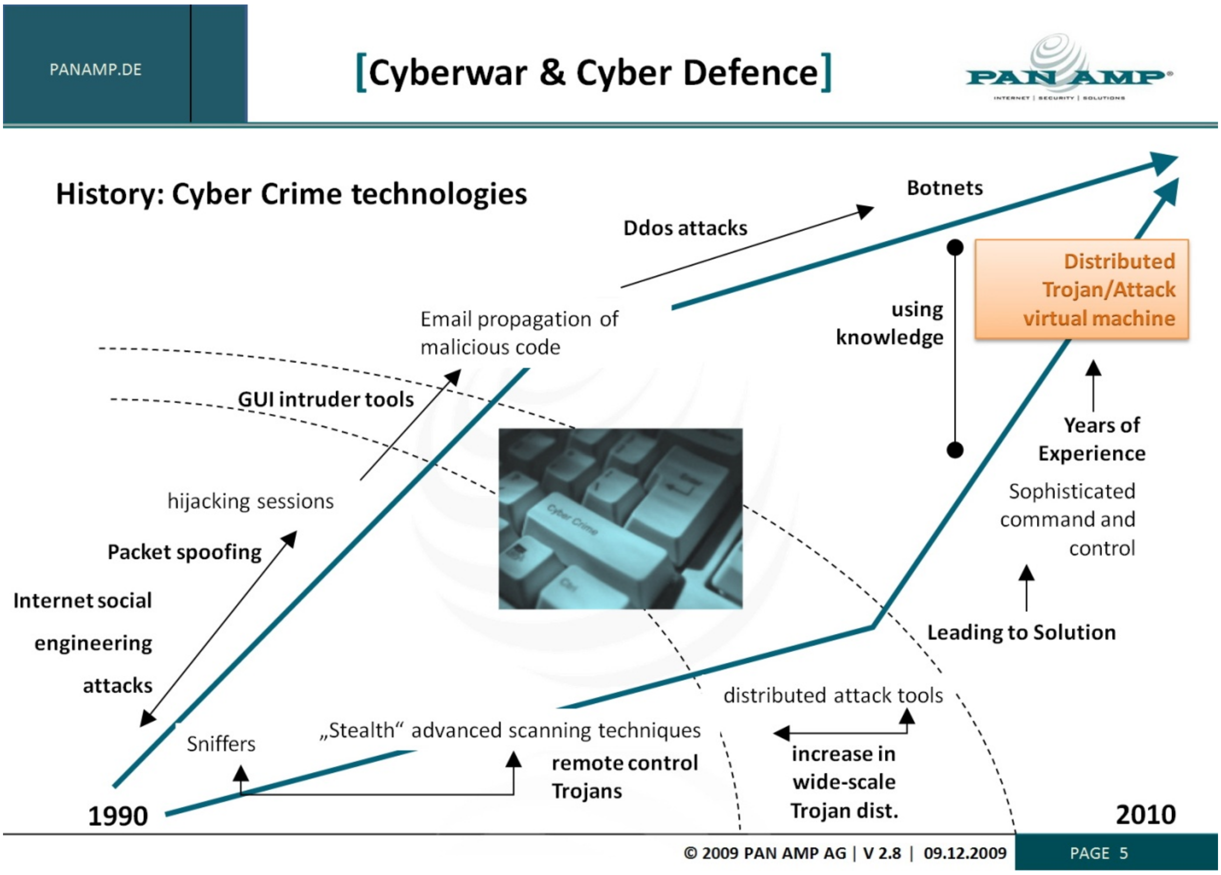
It was at the request of Dr Karl von Wogau, who presided the European Parliament's Sub-Committee on Security and Defence (2009), that I began to prepare my lecture on "Cyberwar and Defence" for the 8th Congress on European Security and Defence held in Berlin on 08 and 09 December 2009. I started by researching 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. Infact, none of the existing assessments and opinions in any of the three sets of information was suitable. Moreover, noranking had so far been established with regard to the seriousness of a cyberwar.

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.

Bert Weingarten, CEO PAN AMP AG, 8th Congress on European Security & Defence (09. Dec. 2009). [Foto: Klaus Dombrowsky]

Physical attacks, such as the destruction and sabotage of hardware (e.g. cables, antennas, and satellite connections) are not part of a cyberwar either, in so far 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.



PANAMP.DE

[Cyberwar & Cyber Defence]

History: Cyber Crime technologies

Botnets

Ddos attacks

Distributed Trojan/Attack virtual machine

using knowledge

Email propagation of malicious code

GUI intruder tools

Years of Experience

hijacking sessions

Sophisticated command and control

Packet spoofing

Internet social engineering attacks

Leading to Solution

distributed attack tools

Sniffers

„Stealth“ advanced scanning techniques

increase in wide-scale Trojan dist.

remote control Trojans

1990

2010

© 2009 PAN AMP AG | V 2.8 | 09.12.2009 PAGE 5

History of multiplied cybercrime technologies (1990 - 2010). [Speech-SecDef-Page 5_20091209]

The Estonian Case

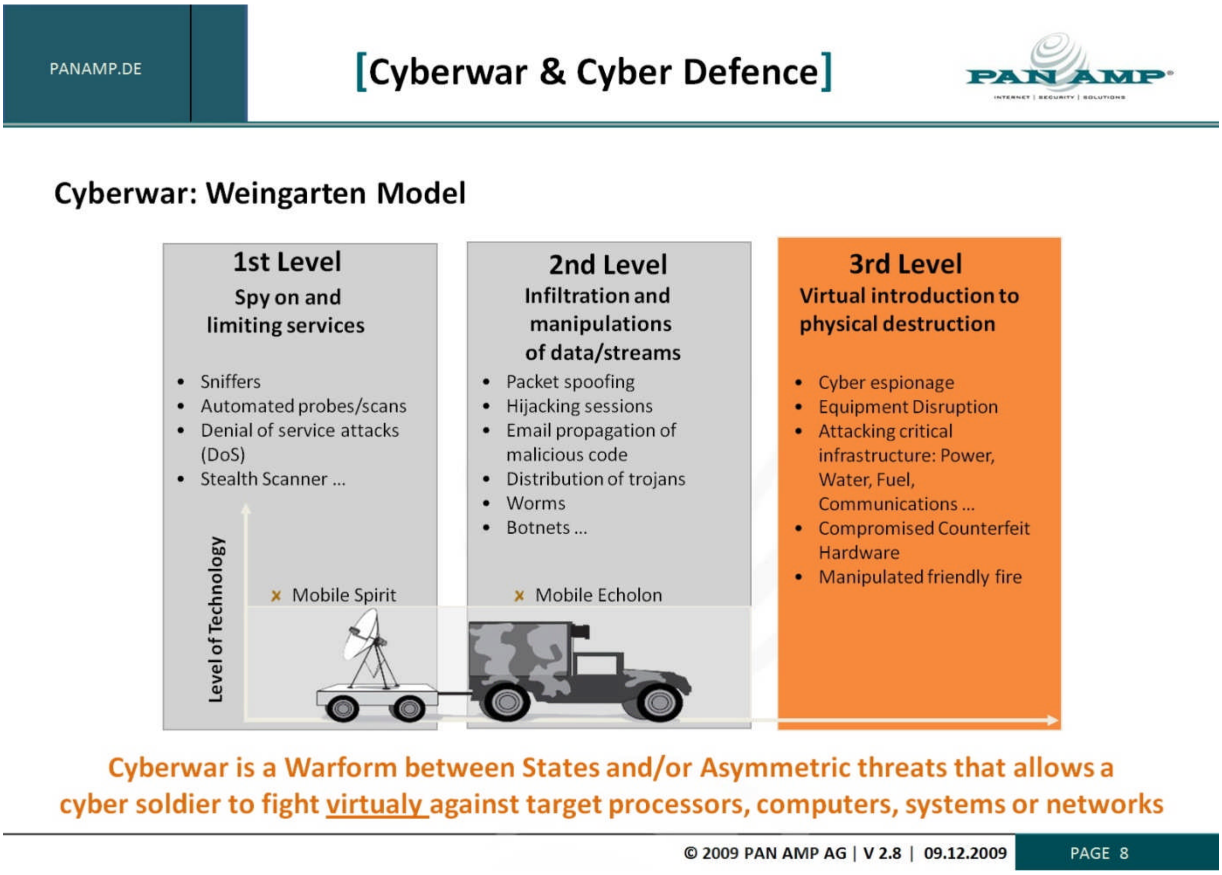
Close study of analyses of the events in Estonia in 2007, and of comprehensive data on individual incidents and interpretations, for which I must thank Vice-Admiral Tarmo Kouts, MoP, (Head of the Estonian delegation to the ESDA/WEU Assembly), Tallinn, led me to conclude that they constituted an example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

Cyberwar is conducted between States, and/or asymmetricthreats, 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.



PANAMP.DE

[Cyberwar & Cyber Defence]

Cyberwar: Weingarten Model

1st Level
Spy on and limiting services

- Sniffers
- Automated probes/scans
- Denial of service attacks (DoS)
- Stealth Scanner ...

2nd Level
Infiltration and manipulations of data/streams

- Packet spoofing
- Hijacking sessions
- Email propagation of malicious code
- Distribution of trojans
- Worms
- Botnets ...

3rd Level
Virtual introduction to physical destruction

- Cyber espionage
- Equipment Disruption
- Attacking critical infrastructure: Power, Water, Fuel, Communications ...
- Compromised Counterfeit Hardware
- Manipulated friendly fire

Cyberwar is a Warform between States and/or Asymmetric threats that allows a cyber soldier to fight virtualy against target processors, computers, systems or networks

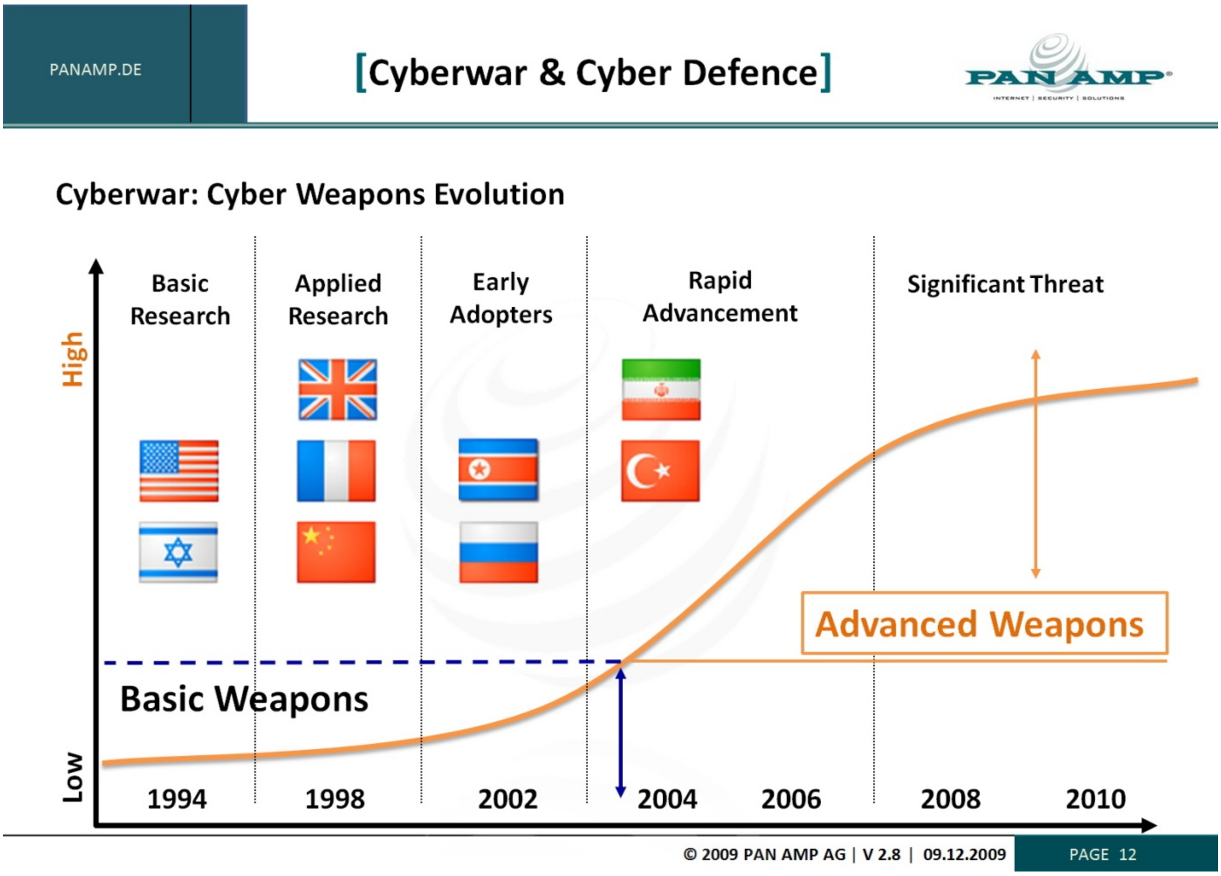
© 2009 PAN AMP AG | V 2.8 | 09.12.2009 PAGE 8

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 betaken 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 maybe manipulated from a distance in order to take over, or take out, enemy units.

Cyberwar: Weingarten Modell, including a level ranking to the seriousness of a cyberwar. [Speech-SecDef-Page 8_20091209]

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".



PANAMP.DE [Cyberwar & Cyber Defence]

Cyberwar: Cyber Weapons Evolution

© 2009 PAN AMP AG | V 2.8 | 09.12.2009 PAGE 12

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 seriousthreat to Europe for, in today's world, the systems needed to conduct cyber attacks 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 in evitable 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.

Cyberwar: damage by the impact of a cyberwar. [Speech-SecDef-Page 8_20091209]

Conflict situation: Cyberwar

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.

Be prepared for Cyberwar

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.

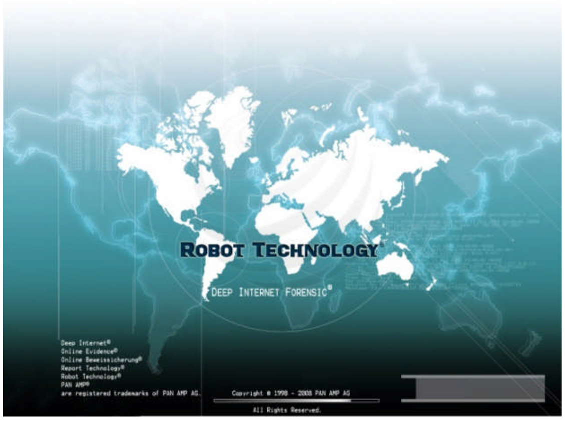
Cyber Defence

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 countermeasure".

Further informations

The area „Cyber Defence", at PAN AMP AG, is developing technologies and systems for military defence of the virtual environment.



Further informations and documents concerning the topic Cyberwar & Cyber Defence are available for download at: www.panamp.de

Contact

PAN AMP AG
Ausschläger Elbdeich 2
D-20539 Hamburg
Tel.: +49 (40) 55 30 02 - 0
Fax : +49 (40) 55 30 02 - 100
E-Mail: info@panamp.de
Internet: www.panamp.de