Editorial: On IRIE Vol. 20

Cyber warfare - when we planned this issue already some time ago we thought of being once again on the leading edge of reflecting the implications of ICTs on global society and our modern life. And once again we have been surpassed by reality.

At first, if we look at the various physical war zones of today we can see more and more cyber weapons in place and in heavy use as well. Nearly every warring party blames the other of using means of hacking to conduct sabotage or espionage in the course of the physical acts of war. And yes, you can bomb the power plant of your opponent or 'stuxnet' it – and of course as the missile can be misguided the virus could also infect the IT infrastructure of a hospital instead. No, a cyber war is not a clean war by definition. But then, what is the difference of killing a combatant with a gun or by a click?

Yet, much more attention has been drawn to the debate of cyber warfare where there is no physical war taking place at all. China and the US e.g. are not at war with each other (at least in the classical sense of having diplomatically declared it to be so or having crossed each other's borders with armed forces wearing uniforms). But in the cyber sphere they do cross their virtual borders all the time and they do attack each other. Let us not be naïve: it is not that they just suspect or blame each other to do so (what they extensively do) – as a matter of fact they are if not yet at war at least testing their capabilities and continuously increase them. Even if the scale is yet more comparable to shooting bullets across the border than to deploying heavy artillery but yes, we have entered this new dimension of the digital sphere now also in the area of warfare. And according to the rising budgets spent every year to improve the effectiveness as well as the camouflage of the respective techniques one can easily foresee their growing importance and also assume their probable social dominance one day.

And that leads to what finally makes the debate red-hot at the very moment: the threats of cyber war or even cyber armament for the civil society also in times and zones of alleged peace. In the name of defending against terrorism and counter espionage and being prepared for possible physical and cyber attacks the super powers have launched an unprecedented ICT infrastructure of mass surveillance and control and do not hesitate to use it also against friendly nations as the NSA scandal made publically clear. Our privacy is under attack by military forces at the very moment. And one could ask if this happens for a greater good. But that only confirms that it happens.

So if cyber war has become a reality even if on a very small scale that one wouldn't call a war yet and if the means of cyber warfare do not stop at concerning also the civil society what is more demanding than asking for ethical reflection of these developments. For the very interesting yet not calming answers please see for yourself in this issue - small in size but rich in content.

Yours,

the editors.

ISSN 1614-1687