ISODARCO – 18th Winter Course
Constructing Security in Europe after Madrid

Security and the European Cyberspace

Giampiero Giacomello

Abstract

Given a geographical connotation ("European") to cyberspace seems like a contradiction in terms: cyberspace is supposed to transcend boundaries. Well, in theory yes, but in practice governments, with the resilience that characterizes them, have found ways to "bring some geography back to cyberspace". China has created the "Great Wall of China" to monitor what dissidents do, Arab countries block messages coming from Israel and France managed to convince the California-based Yahoo! to stop selling Nazi memorabilia to French users. That said, governments, especially democratic ones, have also experience that their control of computer networks can be very limited. Blocking access for normal users is one thing, fighting cybercrime or cyberterrorist is a serious challenge that no single state can hope to pursue alone.

After September 11 2001 , the Unites States has lead the effort to coordinate policies in cyberspace: several countries have signed the Council of Europe Convention on Cyberecrime (although not as many have ratified it yet). After March 11 2004, the Europeans have found out that coordination based on the Convention is fine for independent, sovereign states but it is probably not enough for the highly integrated members of the European Union. Thus they had to probably foster their cooperation on securing cyberspace to a level that is comparable with other EU policies like environmental protection or food safety. Indeed, the European Security Strategy document of December 2003 specifically states that "no single country is able to tackle today's complex problems on its own".

It is interesting to note that, much as the Europeans have struggled to distinguish themselves from the United States when it comes to the "war on terrorism", partially to reinforce their "identity" (i.e. "we're not Americans"), and partially because their experience with terrorism has been different from that of the United States (and ostensibly Russia). Nonetheless, when it come to "talk security", official European documents appear to be using the same language (such as threat analysis or mission oriented capabilities) that are typical of the defense jargon of the United States. If this is the case, such attitude will not only have consequences for the policy-making process in the field of European security, but also, for the type of choice the Europeans will make when it comes to fight cyberterrorism and cybercrime. Until 9/11 (and for some time even after that), in fact, Europeans have considered cybercrime a far greater menace than cyberterrorism (although this distinction was often blurred). Quite logically, Europeans thought that it was a task that mostly fell on the shoulders of law enforcement agencies (with some support from intelligence services) certainly not a matter for "national security" (although, at times, Europeans governments used this rhetoric the way Americans and Russians have done). This position, which made all the more sense if one

consider that most (up to 80-90%) of national information infrastructures is owned or operated by the private sector, slowly began to change after 9/11.

More specifically, this paper/presentation will address two main questions: (a) after March, 11, what have European governments done to protect their information infrastructures and to foster intelligence gathering and counter-terrorism in cyberspace? And (b) why there is still a "European approach" to fight terrorism in cyberspace, given the rising similarities with the American security discourse?

To answer (or, rather, begin to answer), in the paper/presentation I will consider four (short) case-studies:

(a) the signing and ratifying of the **Council of Europe Convention on Cybercrime** (what countries participated and who has, thus far, ratified it)
(b) the formulation of the **European Security Strategy** (who did it and why? What is the rhetoric behind it?)
(c) the development of the **European Security Research Area** (ESRA) (when did it appear? Who are the main actors involved, thus far?)
(d) the launch of the **European Network and Information Agency** (ENISA).

At this early stage, this paper/presentation (PowerPoint) should clearly be intended as an exploratory work, based on an inductive approach. Thus, more than conclusions, some working hypothesis should be expected. In fact, time permitting (and research funds), a few more points could be added and can certainly come up during the 45 min. Q&A session.

These might include:

(e) **Europol**, the European Police Force (which, at the time of writing has no supervision from European elected body, but only from member governments);
(f) **Eurojust**, the European body which supports investigations and prosecutions by the member states into "serious cross-border or transnational crime" (given this definition, fighting cybercrime, should thus pertain to Eurojust);
(g) a (still mysterious) **European Centre for Disease Prevention and Control** (ECDC), which should be established in 2005 and will prioritize the coordination of efforts "to improve surveillance, notification, response, assistance, communication and laboratory capacity on health security matters";
(h) finally the new role of the European Union's first **anti-terrorism czar**, Gijs de Vries.

While the caveat expressed above applies, it is fairly easy to conclude that if one examines the kind of "technical" jargon that the EU has used in all these instances, when it comes to security, Europe seems determined to follow the example of the United States. And if this is the case, what will the effects on the perception of Europe as a *Zivilianmacht* (or the "metrosexual, superpower") be? The ISODARCO Winter School is an excellent setting to begin the discussion on such important topics.