The Saint-Cyr Chair of Cyberdefence and Cybersecurity, Sogeti, Thales organized a symposium on Wednesday (May 14th) on the theme "(Re)building cyberconfidence amongst partners and allies." In an international context where states, companies and groups of individuals use massive amounts of data for strategic purposes, stakeholders attempt to shed light on the crucial question about rebuilding cyberconfidence amongst partners and allies within a legal framework, which is to date uncertain.

State security is in a large part based on technical intelligence and more specifically on signals intelligence. This is even truer for Anglo-Saxon countries since September 11th. Edouard Snowden's revelations about the existence of systems and processes for surveillance (like PRISM, Quantum, and signals intelligence SIGINT), which are active and legal under American law, shook the confidence of traditional partners and allies. However, with growing threats of cyberterrorism, cyberwarfare and cybercrime, allies are forced to work together to protect themselves. Restoring trust is a *condicio sine qua non*. It can only be restored with inter-State agreements and international legislation. In the face of cyberthreats, the challenge is to find a balance where national security is guaranteed while respecting the privacy of citizens. On a legal level, France and more generally Europe differ from the United States, at the risk of being cut off from the rest of the world. Despite national and European will to protect individual freedoms and to anticipate risks in cyberspace, laws must be inevitably adapted to fit the overall interconnection of systems and individuals; this is an issue that we cannot escape.

History teaches us that alliances are created to help face adversity and common threats. The same is true in cyberspace, while these alliances are closely connected to the interests (in particular economic ones) of countries. They are used to build capacity against common threats, and to lead allied counties to adopt a shared vision and understanding of the world. However, the need to communicate and therefore to divulge information with each other may not be reasonably done in an apparatus as large as Europe, made up of countries with different cultural or economic interests. Partnerships are easier and therefore more realistic on a bilateral basis. France can play a major role in the organizing of the cyber domain in the future. In order to do so it must go beyond the confidence crises as we are now experiencing, and work on innovative, secure and scalable commercial solutions integrated upstream in information systems. Using the dynamic private sector and taking a long-term partnerships approach, it is at this price that France can remain a credible ally internationally.

This seminar highlighted the major challenges brought about by cyberspace across its dimensions: societal, legal, diplomatic and commercial. Establishing a climate of trust and security between the private sector partners and the Defense is a priority; the Chair of Cyberdefense-Cybersecurity intends to contribute to this.

The Chair thanks its partners