IESUE/SEM(09)04

10 March 2009

Jean-Pascal ZANDERS

INSTITUTE REPORT

Seminar on

CYBER SECURITY: WHAT ROLE FOR CFSP?

organised jointly by General Secretariat of the Council of the EU
& the EU Institute for Security Studies in cooperation with Estonia
held in Brussels on 4 February 2009

Introduction

The seminar entitled 'Cyber Security: What Role for CFSP?', organised jointly by General Secretariat of the Council of the EU and the EU Institute for Security Studies in cooperation with Estonia, was held in Brussels on 4 February 2009. More than sixty representatives from EU Member States, the EU Council Secretariat, the European Commission, the European Parliament, the EU Institute for Security Studies, research institutions and non-governmental organisations participated.

Cyber security was identified as a security issue in the report on the implementation of the European Security Strategy (ESS) submitted by SG/HR Javier Solana to the European Council in December 2008. The seminar's goal was to initiate a first discussion (brainstorming) on the implications for the EU of the cyber security agenda and related threats; to raise subject awareness, and to identify a number of critical issues for the possible development of a policy under the Common Foreign and Security Policy (CFSP) that would be a part of a comprehensive approach by the EU in this area.

This report summarises the main points of the discussion and considerations for policy development.

Threat perceptions

Cyberspace has become a central aspect of our way of life, bringing economic and personal opportunities that were unimaginable only a decade or two ago. However, the world's growing dependency on information and communication technologies also brings vulnerabilities. Different types of cyber attacks have taken place in recent years; reaching from the planting of malicious software on personal computers and the defacing of public websites to the penetration of databases and secure communication networks and well-coordinated, massive attacks against national critical infrastructure and public institutions of the EU Member States. Individuals, organised crime and terrorist entities may all be involved, but there is also growing evidence that politically motivated attacks are being carried out by state-inspired or state-sponsored entities but also by government agencies. Cyber attacks may also be launched prior to or in support of military operations. Successful penetration into the computer systems of military forces can debilitate entire operations, forcing military assets and systems to stand down from service while the problem is being addressed.

In cyber-warfare location does not matter. Several participants noted that state-sponsored cyber attacks against another state can be launched from anywhere. Sufficient software solutions, including tools available from the growing malware (black) market, are available to disguise the origin of such actions or prevent counter-measures.

Some speakers and participants viewed so-called failed states as a particular source of concern, because the rapidly expanding information networks remain highly unregulated and weak governments, conflicts and wars preclude serious monitoring efforts and law enforcement. Stronger states, on the other hand, might loose some of their credibility and legitimacy if they fail to control, regulate and protect that part of cyberspace for which they are responsible.

Counter-measures

Cyber space is highly unregulated and has no control mechanisms in place except for voluntary service interruption to prevent or disrupt an attack. One consequence is that it is very difficult to determine who is behind a particular attack. Having an international regulatory framework in place was viewed as critical to cyber security. Common standards of behaviour and a shared legal framework to address cyber attacks mean that individuals, groups, institutions but also states can be held more accountable. Inter-regional approaches and action on legal, technical and procedural aspects form part of package of measures. Nevertheless, different countries are likely to maintain different principles. Therefore there is a need to first seek out those elements for an international regulatory framework on which consensus can be relatively easily achieved. Updating legislation was seen as a major step towards addressing cyber threats.

It was argued that while cognisance of the hierarchy of measures is important, the responses should address the different threat levels simultaneously. Participants thus emphasised that preference should be given to a structured response (at individual, group or state, regional and global levels) that somehow corresponds with various threat levels in cyberspace.

From a purely military standpoint cyber space could be seen as fifth domain of defence, alongside land, sea, air and space. It follows that corresponding capabilities should be developed too. However, the status of a major cyber attack also remains unclear: should it, for instance, be viewed as aggression covered under Article 51 of the UN Charter; should Article 5 of the NATO

Treaty or the solidarity clause in the Lisbon Treaty be invoked? Particularly in the light of the difficulties to attribute an attack, individual or collective military responses to cyber attacks remain unclear. A possible military response should therefore only be considered as part of a more comprehensive approach.

EU policies

Public diplomacy is a core element of the EU's distinctive approach to security and should take up a central place in its approach to cyber security under the CFSP. For the EU it is important to realise that the response to the cyber threat should not be limited to the collective action of the 27 Member States, but also involve the active engagement of other partners and relevant international institutions.

Participation in and developing international legal regimes is another aspect that can be undertaken under the CFSP. (Today only some EU Member States are party to the Council of Europe's Convention on Cybercrime.) The international legal framework also includes bilateral agreements. However, as the multitude of agreements is likely to lead to contradictions or mutual incompatibility, it may be advisable to aim for a global framework. Once such an agreement is concluded, the parties should turn to the transposition of its provisions into domestic law in order to make the treaty practically enforceable.

Central to the development of possible EU cyber security policy will be the development of a cyber security strategy by the EU or a common operating vision, which brings together agencies, procedures, etc. Several suggestions were made with regard to the creation of an EU Cyber Security Coordinator. Alternative options included an EU Cyber Security Council or an EU Cyber Security Agency, based on the European Network and Information Security Agency (ENISA). Nevertheless, some concerns were voiced about the proliferation of specialised institutions to address each emerging threat, which in the end is unsustainable. On the other hand, there exists a real risk that in the light of the fast evolving security threat the EU's response will be too slow, particularly if attempts were to be undertaken to formulate an EU-wide general policy. One alternative would be to investigate which EU organs have responsibilities relating to cyber security and charge the most central organ with overall responsibility. Another, more decentralised option seeks to maximise and combine the contributions to cyber security of each of the EU institutions and agencies.

While the participants did not question the need for a common EU approach, some discussants noted the relevancy of Member States developing their national strategies in addition to possible EU regulations. There is the option of subsidiarity, whereby the EU first undertakes to protect its own critical infrastructure and then offers assistance, expertise and advice to the Member States. Some participants felt that the primary response and responsibility to address cyber threats lies within the Member States. The discussion also touched upon the active engagement of the private sector within the Member States. Many stressed that private-public partnership is an essential element of the counter measures by the EU Member States.

At the grass roots level the importance of cooperation between the EU Member States´ Computer Emergency Response Teams (CERTs) was mentioned. It is essential not only to engage them to more structured cooperation with their own governments, but also to study if such cooperation could be established at the EU level.

International cooperation was another focal point of discussion. Cooperation with international organisations, such as the UN, NATO, OSCE, International Telecommunication Union (ITU), Council of Europe and regional groupings and initiatives (e.g., ITU's IMPACT), should be enhanced. It was also suggested that the EU might consider transatlantic cooperation with the USA, which has already set up several major cyber security initiatives. EU cooperation with NATO, which has a cyber defence policy since the autumn of 2007, proceeds with well-known limitations.

There may be a certain role for the EU military structures or European Defence Agency (EDA) to define an EU defence policy, but this requires clarification. The issue, however, cannot be ignored as a number of cyber attacks were directed against the EU as a whole. Opinion varied as to whether a single global shield or a multitude of initiatives (national, EU together with other regional initiatives) are the better way ahead. Many participants preferred a combined approach: doing what is possible domestically and regionally, while working in parallel with third countries and taking steps to build up a global consensus.

Another dimension of EU policies in the domain of cyber security is the prevention of the securitisation of core values core values such as freedom of access to information and freedom of expression. While it was recognised that both freedoms could mean different things in different societies, in global efforts to address the cyber threat the EU ought to promote those core values and not compromise on them. The view was expressed that democratic governments have voluntarily accepted certain limitations on freedoms in order to be able to adequately address threats.

Considerations for policy development

It was also stressed that the response at the state level requires first of all and most importantly political will but also technical innovation, structural changes, and organisational reforms and updating of legislation. At the Union level sizeable efforts to address cyber threats are already taken under the First and Third Pillars. The central question at the seminar was whether to address the cyber threat under the Second Pillar too and to seek a more comprehensive cross-pillar approach. Although the seminar did not aim to formulate concrete policy recommendations, the discussions revealed a number of critical issue areas that should be addressed in the early stages if development of a cyber security policy under the CFSP is desirable:

- There is a clear need for conceptual clarity and precise terminology. This is particularly relevant with regard to the identification of the types of cyber threats and issues relating to cyber security (prevention, defence, remediation and law enforcement, among other things) that will be addressed under the CFSP.

- Vulnerability of the cyber space needs to be catalogued. There is also a need to consider whether cyber security threats originating from abroad should be treated as a criminal or political or defence matter under the CFSP.
- Building on the two previous points, the highest policy-making levels in the EU Member States should receive thorough briefings on the core substance of the cyber threats in order to have a common understanding concerning the moment and type of action that should be taken.
- Addressing the security challenges in cyber space dissolves the boundaries between internal affairs, foreign policy and defence, and a comprehensive EU response is likely to cross the respective pillars of the Maastricht Treaty.
- On an international level, there are very few international treaties and conventions dealing with the subject. All EU Members should be actively encouraged to become party to the Council of Europe's Convention on Cybercrime. The EU could do more to promote the development of a common legal framework and common standards worldwide, including the possible framing of a binding universal convention on the use of cyber space.
- Freedom of access to information and expression are among the core values of the EU Member States. In order to prevent their securitisation, the cyber threats need to be carefully circumscribed and a meaningful democratic debate held on the implications of the specific security measures being proposed.
- Law enforcement plays a central role in the organisation of cyber security. This means that EU Members should have adequate national legislation in place, which includes information security standards for individual and corporate users. It also means that international treaties should be promoted to establish common legal standards. This is an area where the EU can develop initiatives under the CFSP.
- Because most of the cyber attacks to date are suspected to originate from third states, adding cyber security clauses to EU agreements with third states along the same lines as those covering counter-terrorism, was also suggested. The EU should engage these countries in dialogue and encourage updating of their legal instruments with regard to the cyber dimension. In this area the EU could set up assistance programmes for developing countries to help them achieve the international standards in support of global cyber security.
- Raising public awareness on all levels will remain an essential part of any follow up activities by the EU is this area.
- Information concerning the EU Member States´ leading agencies dealing with this issue and the measures they use could be collected, catalogued and analysed with the aim to create a pool of best practices.
- On a practical level a commonly shared vocabulary, terminology and frequently asked questions analogy could be elaborated.
- The Critical Information Infrastructure Protection (CIIP) was identified as another area where EU Member States´ individual efforts and the EU collective action could be combined and further developed. The European Commission announced that a communication on this subject will be available in March.