Briefing

June 2015

European Parliament

Cybersecurity and cyberdefence

EU Solidarity and Mutual Defence Clauses

SUMMARY

Faced with an increasing number of complex crises with a trans-border dimension, the European Union has invested significant energy and resources in strengthening its crisis- and disaster-management capabilities. To that effect, the Treaty of Lisbon equipped the Union with two provisions aimed at improving the EU's response to natural or man-made disasters (the Solidarity Clause) and military aggression against an EU Member State (the Mutual Defence Clause).

For some time, both clauses remained purely theoretical concepts, without clear rules regarding their activation or procedures once either of the two is invoked by a Member State. In 2014, after many months of discussion, the Member States agreed on arrangements for the implementation of the 'Solidarity Clause'. The 'Mutual Defence Clause' has yet to see similar progress. Whether backed by procedures or not, so far the Member States have been reluctant to make use of either of the two provisions.

Many areas of human activity are increasingly dependent on information technology. At the same time, over the past year some major media outlets and companies – including Sony and TV5 Monde – have become victims of cyber-attacks. Consequently, policy-makers are increasingly preoccupied about the risk of cyber-attacks with disastrous consequences for critical national infrastructure. Given the interconnectedness between the Member States and their inherent limitations to tackle a complex disaster provoked by a cyber-attack alone, there is some debate about the likelihood of the Solidarity and Mutual Defence Clauses eventually being invoked. The European Parliament has addressed these issues on three different occasions but its role once any of the clauses is activated remains to be defined.

In this briefing:

EPRS | European Parliamentary Research Service

Author: Patryk Pawlak

Members' Research Service

PE 559.488

EN

Background

Faced with complex crises, the European Union (EU) has made significant efforts to improve its response capacities, including the adoption of the EU Integrated Political Crisis Response (IPCR) arrangements and the transformation of the Monitoring and Information Centre (MIC) into the Emergency Response Coordination Centre (ERCC) in 2013.[1] Solidarity and Mutual Defence Clauses were introduced in the Treaty of Lisbon – Articles 222 TFEU and 42(7) TEU respectively – to strengthen cooperation between Member States and the EU institutions in case of a crisis or armed aggression respectively.[2] The Solidarity Clause goes further by creating an obligation on all Member States to act jointly and to assist one another in the event of disasters and crises which exceed their individual response capacities.[3] While the Treaty provision concerning the Solidarity Clause has been supplemented with more detailed implementation guidelines – thus providing a more operational meaning to the concept – the Mutual Defence Clause remains a rhetorical concept and its implementation still needs to be defined.[4]

With many areas of human activity being heavily dependent on information technology on the one hand, and a growing number of security breaches on the other, there is a tangible risk of a cyber-attack resulting in a large-scale disaster. The possibility of employing the Solidarity Clause to mitigate the damage of such an attack has been mentioned in a number of cyber-related documents, even though neither the Treaty articles nor the decision on the arrangements for the implementation by the Union of the Solidarity Clause make explicit reference to cyber-attacks, but only to the more broad concept of man-made disasters. The EU Cyber Security Strategy proposed jointly by the European Commission and the High Representative in February 2013, tackles the question of EU support in case of a major cyber incident or attack. According to the Strategy, 'a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause'. In addition, the June 2013 Council Conclusions on the Cybersecurity Strategy of the EU, welcoming the proposed Strategy, invite Member States 'to take into account cybersecurity issues in light of ongoing work on the solidarity clause'. Furthermore, the EU Cyber Defence Policy Framework adopted by the Council in November 2014 states clearly that 'the objectives of cyber defence should be better integrated within the Union's crisis management mechanisms. In order to deal with the effects of a cyber-crisis, relevant provisions of the Treaty on the EU and the Treaty on the Functioning of the EU may be applicable, as appropriate'. Both the Solidarity Clause and the Mutual Defence Clause are mentioned explicitly in the footnote and could potentially be activated. It is important to note, however, that activation of the Solidarity Clause would occur to deal with the consequences of a cyber-attack and not the cyber-attack itself.

Understanding the nature of a (cyber) crisis

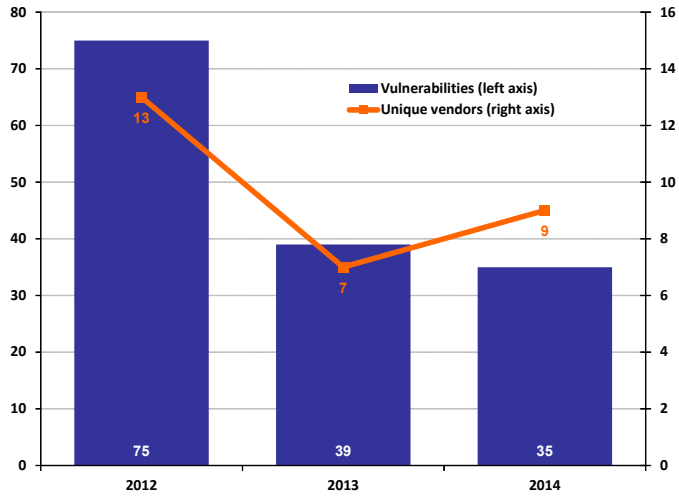
As digital networks now constitute the backbone of our societies' functions (i.e. financial systems, energy infrastructure and communication tools), there is a risk that organised criminal groups or foreign governments will exploit their vulnerabilities. Many countries have included the protection of critical information infrastructure in their national security strategies. Therefore, strengthening the security and resilience of critical infrastructure against cyber-threat is a priority on policy agendas, including with regard to crisis management.

According to United States intelligence, only a limited number of countries have the capacity to invade and possibly disable the computer systems of power utilities,

financial institutions or aviation networks. Numerous studies conducted by private and public institutions argue that the risk of cyber-attacks on critical infrastructure exists but a large-scale attack is unlikely to materialise. A report released in February 2015 by US Intelligence, confirms that, rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, there will be 'an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security'.

However, there is no consensus on a globally agreed threshold above which a series of cyber incidents would be considered a crisis, which is one of the issues currently being debated by the UN Governmental Group of Experts. The EU Agency for Network and Information Security (ENISA), for instance, defines incident as 'an event which can cause a breach of security or a loss of integrity of electronic communication networks or services'. Some experts underline that, because cyber-incidents are common and hardly ever reach the level of a full-blown cyber-crisis (i.e. an abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability); they are not addressed at the strategic level unless a crisis is imminent.[5]

Figure 1 – Vulnerabilities disclosed in industrial control systems



Source: Symantec.

In the EU, substantial competence in this regard remains with national authorities. According to the EU Standard Operational Procedures (EU-SOPs), developed by the EU and European Free Trade Association (EFTA) Member States, in collaboration with ENISA, and adopted in February 2014, each country defines what sort of event or series of events, natural or man-made, constitutes a cyber-crisis. In the case of a multinational cyber-crisis, the causes or impact need to concern at least two countries. Through a combination of contact points, guidelines, workflows, templates, tools, and good practices, the EU-SOPs generate shared technical and non-technical knowledge, which then allows for a better understanding of the context and identification of effective action plans. In addition, the EU's response capacity – including at a technical, political and operational level – is regularly tested through cybersecurity exercises like 'Cyber Europe 2014', completed in early 2015.

Nevertheless, the risk of computer-based attacks on critical infrastructure – defined as 'those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States' – exists and cannot be ignored due to their potentially high impact. These could include attacks on energy infrastructure, healthcare institutions, water and food supplies, or other industries which rely on internet networks. Most of these facilities and services rely on Industrial Control Systems (ICS) which are

responsible for monitoring and controlling industrial processes such as electricity distribution, water treatment or management of transport networks.[6] Following a decade-long transformation process, ICS systems have evolved from isolated systems to open architecture and standard technologies, which expose them to cyber-attacks like any other computer connected to the internet (see Figure 1).[7] For instance, upgraded electricity networks facilitating two-way digital communication between supplier and consumer, allowing for more efficient transmission and distribution of electricity – also known as smart grids – are vulnerable to rogue codes in the software or remotely operated 'kill switches' and hidden 'backdoors' on hardware.[8] Cyber-attacks such as Stuxnet in 2010, cyber-espionage campaigns like Dragonfly, and the targeted malware campaign, Sandworm, in 2014, demonstrate that attacks against ICS have matured and are becoming more frequent.[9]

The EU has taken a number of steps to reduce the vulnerabilities of critical infrastructure due to their networked nature. In 2009, the European Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP) entitled 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'. Recognising that many critical infrastructure platforms rely on information and communication technologies, the Communication aimed at ensuring a high level of preparedness, security and resilience capability, both at national and EU level. Two years later, the Commission took stock of the implementation and concluded that purely national approaches to tackling security and resilience challenges are insufficient, and announced follow-up actions in the Communication on CIIP on 'Achievements and next steps: towards global cyber-security'. The proposed Network and Information Security (NIS) directive, put forward by the Commission on the same day in 2013 as the EU Cybersecurity Strategy aims to further strengthen a number of elements in the EU's preparedness and response capacity, including improving cooperation between various stakeholders (public and private sector, Member States), while at the same time obliging critical sectors to adopt risk management practices and report major incidents. The proposal received its first reading in April 2014, in the outgoing Parliament. Negotiations between the EP (rapporteur Andreas Schwab, EPP; Germany) and the Council are continuing with a view to concluding an early second reading agreement.

Solidarity Clause

Legal framework

The EU Solidarity Clause was introduced with Article 222 of the Treaty on the Functioning of the European Union (TFEU), which states that:

> *The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to … assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster*.

For a long time, there was no clarity on how the invocation of the Solidarity Clause would work in practice and what would be its implications. After many months of discussion in a 'Friends of the Presidency' Group, the Council adopted rules and procedures for the implementation of the Solidarity Clause in June 2014. The Council Decision (2014/415/EU) clarifies the definition of the concept of a 'disaster' in the

context of Article 222. It is defined as '... any situation which has or may have a severe impact on people, the environment or property, including cultural heritage'. The same document defines 'crisis' as 'a disaster or terrorist attack of such a wide-ranging impact or political significance that it requires timely policy coordination and response at Union political level'. Such a broad definition implies that it would be possible to activate the Solidarity Clause in order to address the consequences of a severe cyber-attack, dealing with the consequences of which would be beyond the capacities of a Member State.

Invocation of the Solidarity Clause

Based on Decision 2014/415/EU on implementation of the Solidarity Clause, the political authorities of the affected Member State may invoke the Clause if they conclude that the crisis overwhelms their response capabilities. The implied condition, however, is that the possibilities offered by existing means and tools at national and Union level have already been exploited. The invocation should be addressed to the Presidency of the Council, and to the President of the European Commission through the Emergency Response Coordination Centre (ERCC), which acts as the central round-the-clock contact point at Union level with Member States' competent authorities and other stakeholders, 'without prejudice to existing responsibilities within the Commission and the HR and to existing information networks'.[10] The Presidency informs the President of the European Council and the President of the European Parliament of the Solidarity Clause's invocation (see the annex). Subsequently, the political and strategic direction of the Union response is ensured by the Council whereby the Council Presidency activates Integrated Political Crisis Response arrangements (IPCR) and provides information to Member States.

The ERCC facilitates the production of Integrated Situational Awareness and Analysis (ISAA) reports – in collaboration with the EU Situation Room and other Union crisis centres – that should allow for a strategic overview of the situation within the Council. The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy are tasked to:

- Identify all relevant Union instruments – including military capabilities – that can best contribute to the response to the crisis, and propose the use of resources within the remit of Union agencies;
- Advise the Council on whether existing instruments are sufficient;
- Produce regular integrated situational awareness and analysis (ISAA) reports to inform and support coordination and decision-making at political level in the Council.

Implementation of the Solidarity Clause by the EU should rely on existing instruments to the extent possible, and should increase effectiveness by enhancing coordination and avoiding duplication. The EEAS contributes to raising situational awareness by providing intelligence and military expertise, as well as through the network of EU Delegations that may also contribute in the response to threats or disasters on Member States' territory, or to crises with an external dimension. Depending on the crisis, relevant contributions may also be required from the EU agencies under the Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP) structures. Nevertheless, the procedures established for the implementation of the Solidarity Clause have no defence implications and are without prejudice to Article 42(7) TEU on the Mutual Defence Clause. It needs to be clearly stated that, even though this procedure has been developed to deal with complex crises in general, it would also

apply *mutatis mutandis* to a possible cyber-crisis, if a Member State decides to invoke the Solidarity Clause.

The EU Integrated Political Crisis Response arrangements (IPCR)

- The IPCR arrangements reinforce the European Union's ability to take rapid decisions when facing major emergencies requiring a response at EU political level.
- The IPCR process is driven by the Presidency, which ensures its political control and strategic direction, with the support of other relevant actors, notably the General Secretariat of the Council (GSC), the European Commission and the European External Action Service.
- The process is centred on Coreper (Committee of the Permanent Representatives of the Governments of the Member States to the EU) and follows existing Council procedures. An informal Presidency-chaired roundtable is established to prepare decisions on the possible handling of the crisis within the Council and to develop proposals for action to be presented to Coreper/the Council.
- The Council-owned web platform is a communication hub. It is accessible to all relevant stakeholders, at Member State and EU levels. The web platform receives inputs and contributions from Member States, the Commission, the EEAS and the EU Agencies.

Source: Council of the European Union, 2013.

Mutual Defence Clause

Legal framework

The Mutual Defence Clause was introduced in Article 42(7) of the Treaty on the European Union and is interpreted as an equivalent clause to Article 5 of the North Atlantic Treaty on collective defence. The Mutual Defence Clause reads as follows:

> *If a Member State is the victim of an armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the UN Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitment under the NATO, which, for those States which are member of it, remains the foundation of their collective defence and the forum for its implementation.*

Consequently, this Treaty provision can be used when a cyber-attack is qualified as an armed aggression. NATO's own 'Glossary of Terms' speaks of 'computer network attack' as 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'. It also includes a note that 'a computer network attack is a type of cyber-attack'. In legal terms, the UN General Assembly defines aggression as 'the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations'. However, establishing in practice whether a cyber-attack constitutes an armed attack, whether it constitutes a legitimate use of force (*jus ad bellum*), and how force may be employed (*jus in bello*), remains contentious among international legal scholars[11] and is one of many subjects being discussed by the Governmental Group of Experts working under UN auspices.

Invocation of the Mutual Defence Clause

While doctrine on the application of the Mutual Defence Clause has not been operationalised to the same extent as the Solidarity Clause, it remains to be seen whether Member States will invoke it in the case of a cyber-attack. The outcome of the 2014 NATO Summit in Wales offers some initial insights. In the declaration adopted at the summit, members agreed that Article 5 provisions can be invoked in the case of a

cyber-attack with effects comparable to those of a conventional armed attack. Given the partly overlapping membership between the EU and NATO – only six EU Member States are not members of the latter, (Austria, Cyprus, Ireland, Finland, Malta, and Sweden) – it is possible that similar reasoning will be adopted for the activation of the Mutual Defence Clause. Nevertheless, even NATO itself has not established any clear procedures or thresholds for the use of Article 5 for cyber defence, insisting that this will be a political decision taken on a case-by-case basis. Such an approach is in line with arguments presented by legal scholars, who argue that damage or destruction of data does not necessarily generate consequences that would qualify them as an armed attack. An automatic acceptance that a cyber-attack constitutes armed conflict would otherwise substantially lower the threshold at which states have a right to use force in their response to actions directed at them.[12]

Another debate concerns the application of International Humanitarian Law (IHL) once the Mutual Defence Clause is activated. Article 48 of the Additional Protocol I to the Geneva Conventions of 1949 requires that parties to a conflict 'at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and direct their operations only against military objectives'. However, whereas such a clear-cut distinction is possible in the real world, it is much more difficult to make in cyberspace where differentiation between civilian and military targets is harder to make and maintain during a cyber-attack. It is therefore argued that if such a distinction cannot be assured, parties to the conflict should be restricted from using cyber-weapons.[13] To test these and similar dilemmas, the EU Cyber Defence Policy Framework suggests adding a cyberdefence dimension to existing scenarios for MILEX and MULTILAYER exercises, and to organise a dedicated CSDP cyberdefence exercise.

Complementary mechanisms

The activation of the Solidarity or Mutual Defence Clause in case of a cyber-attack requires that decision-makers at strategic and political levels are involved in the process. Multinational cyber-crisis management, however, also requires that technical experts work in parallel to detect and prevent cyber-attacks from occurring and/or respond to them and deal with the consequences. For instance, the scenario of the 'table-top exercise' on IPCR and Solidarity Clause conducted in 2014, was based on a series of cyber-attacks – even though the crisis management exercise itself focused on dealing with the consequences and not the cyber aspect. Consequently, the following group of actors may be involved in the process:

- In case of the Solidarity Clause: a national Computer Emergency Response Team (CERT) – also known as a Computer Information Security Response Team (CSIRT) – and/or other designated bodies within national structures, including law enforcement agencies and the private sector. CERTs (or CSIRTs) are each country's primary security provider and the main asset in responding to cyber-attacks. In order to strengthen their response capacities, many CERTs have established regional or global networks like FIRST or Asia Pacific CERT (APCERT).
- In case of the Mutual Defence Clause: a national cyber command or a military Computer Emergency Response Team (milCERT). In response to a growing number of cyber-attacks and a potential use of cyber capabilities in military conflict, a number of countries have either developed or are currently developing their cyberdefence doctrines and capabilities.

Such a division is of course a simplification and clear-cut division lines between civilian and military might be difficult to maintain in a complex crisis. Therefore, many countries and organisations – including within the EU – have developed national cybersecurity strategies which lay out the rules of engagement and principles for cooperation between different stakeholders.

The European Parliament

The European Parliament (EP) has addressed the issues related to the implementation of the Solidarity and Mutual Defence Clauses on three different occasions.

In November 2012, the Parliament adopted two important resolutions in this regard:

- Resolution on the EU's Mutual Defence and Solidarity Clauses: called upon the Member States, the European Commission and the Vice-President/High Representative 'to make full use of the potential of all relevant Treaty provisions, and in particular the Mutual Defence Clause and the Solidarity Clause, in order to provide all European citizens with the same security guarantees against both traditional and non-conventional threats'. Such a broad wording in the resolution suggests that Members also wished to allow for the possibility of these clauses being used in the case of a cyber-attack. It also devotes significant attention to the Mutual Defence Clause itself, by reaffirming that 'the use of force by the EU or its Member States is only admissible if legally justified on the basis of the UN Charter', and that cyber-attacks against critical infrastructure aiming to cause severe damage and disruption may qualify to be covered by the Mutual Defence Clause. Nevertheless, the EP also highlights the need to respect the principle of proportionality.
- Resolution on Cyber Security and Defence: recognised a growing cyber threat to security, defence, competitiveness and stability. The resolution also called upon the Commission and the High Representative to include cyber-attacks in discussions on the arrangements for the implementation of the Solidarity Clause and on the Mutual Defence Clause. In addition, the resolution made a number of concrete suggestions towards improving synergies between cyber-crisis management and crisis management plans in general, including development of national contingency plans, provision of awareness-raising training on cybersecurity (including conducting cyber exercises), and the need for closer coordination between EU and NATO, especially concerning planning, technology, training and equipment.

While these resolutions demonstrate the Parliament's views on the application of the Solidarity and Mutual Defence Clauses, the European Parliament's role once any of the clauses is activated remains to be clearly defined. The arrangements for the implementation of the Solidarity Clause require the Presidency of the Council to inform the President of the Parliament. However, there is no provision on what happens next: either within the European Parliament or between the Parliament and institutions participating in crisis management.

In addition, the Parliament's most recent annual resolution, adopted in March 2015, on the Annual Report from the High Representative of the EU for Foreign Affairs and Security Policy not only called for active promotion of these instruments, but also encouraged Member States to make use of them. Interestingly, the resolution also devoted much attention to developing the industrial and technological resources needed to improve cybersecurity and strengthen the resilience of relevant infrastructure. These points are particularly relevant in light of the ongoing negotiations on the NIS Directive, and for the reinforcement of the EU's role as a security provider.

Main references

Boin, A., Ekengren, M., Rhinard, M., *The European Union as crisis manager. Patterns and prospects,* Cambridge University Press, 2013.

Pawlak, P., Ricci, A. (ed.), *Crisis rooms. Towards a global network?,* European Union Institute for Security Studies, 2014.

Schmitt, M. N. (ed.), *Tallinn Manual on the International Law applicable to cyber warfare*, Cambridge University Press, 2013.

Endnotes

1 Boin, A., Ekengren, M., Rhinard, M., *The European Union as crisis manager. Patterns and prospects,* Cambridge University Press, 2013.

2 In fact, these clauses are not new. The Mutual Defence Clause is based on the 1954 Brussels Treaty that established the Western European Union (which ceased to exist in 2011). Both were also included in the Treaty establishing a Constitution for Europe.

3 A crisis may occur inside or outside EU borders, but must have consequences on EU territory.

4 Article 222 TFEU explicitly instructs the Council to adopt a decision concerning implementation, which is not the case for Article 42(7) TEU.

5 Trimintzios, P., Holfeldt, R., Koraeus, M., Uckan, B., Gavrila, R., Makrodimitris, G., Report on cyber crisis cooperation and management, ENISA, November 2014.

6 Industrial Control Systems (ICS) is a general term encompassing several types of control systems, including supervisory control and data acquisition (SCADA) systems or distributed control systems (DCS). SCADA are the largest subgroup and are vital components of critical infrastructures used to control oil and gas pipelines, electrical power grids or railway transportation. Thanks to the use of standard hardware and software and increased connectivity via the internet, SCADA systems offer many benefits, including: access to real-time data on production operations, more efficient control paradigms, improved plant and personnel safety, and reduced operating costs.

7 ENISA, Protecting Industrial Control Systems. Recommendations for Europe and Member States, December 2011.

8 ENISA, Smart Grid Security. Recommendations for Europe and Member States, July 2012.

9 Symantec, Internet Security Threat Report, Vol. 20, April 2015.

10 ERCC was established by Decision No 1313/2013/EU.

11 Schmitt, M. N., 'Attack' as a term of art in international law: the cyber operations context, 4th International Conference on Cyber Conflict, 2012.

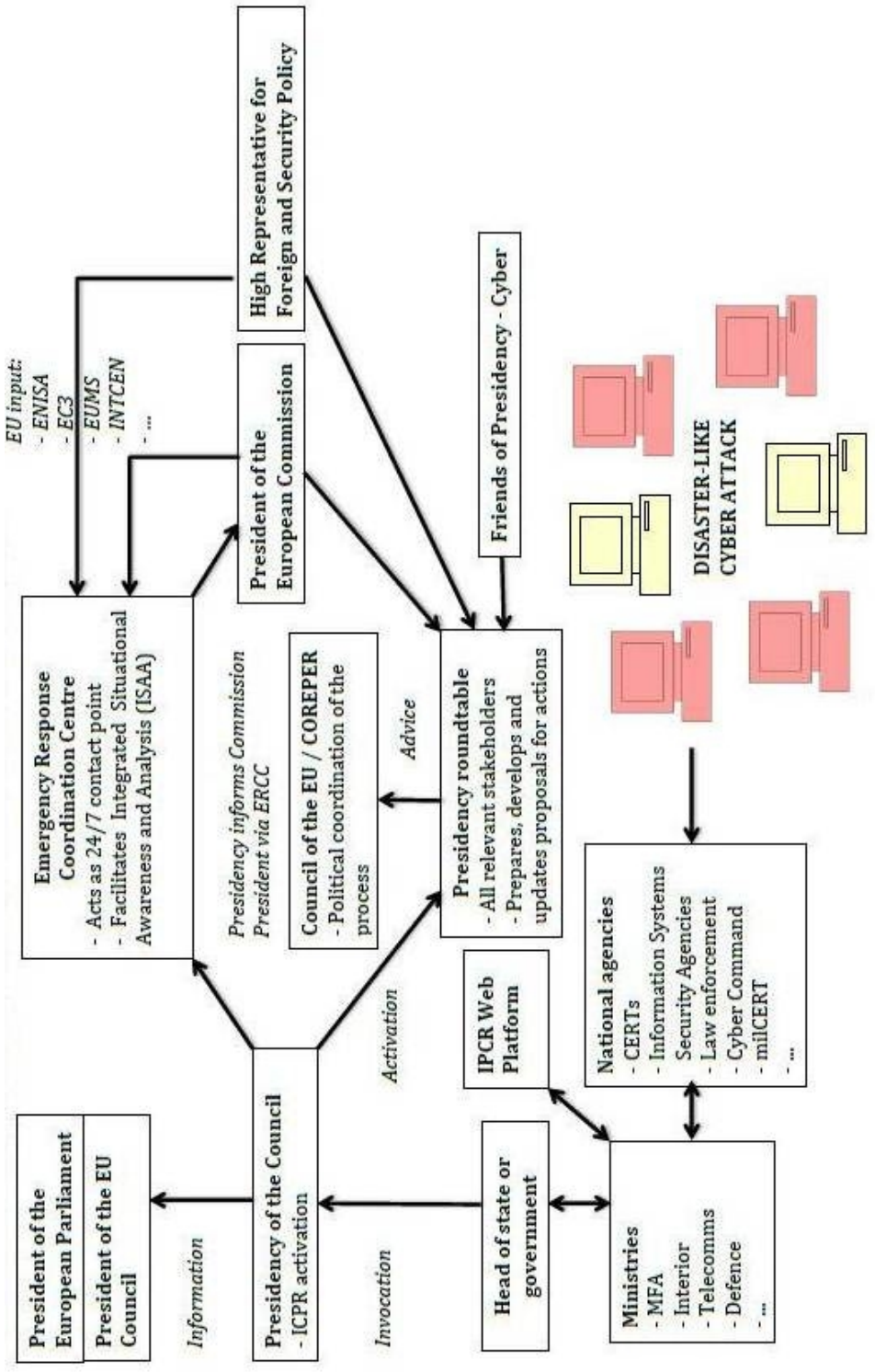
12 Schmitt, M. N., (ed.), Tallinn Manual on the International Law applicable to cyber warfare, Cambridge University Press 2013.

13 Regulations respecting the laws and customs of war on land, 18 October 1907.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Annex: Managing a 'disaster-like' cyber-attack using the Solidarity Clause



Source: Author's own compilation.