THE EU AND GLOBAL CHALLENGES
28 IDEAS FROM THE ERASMUS GENERATION

School of Political Science,
MA in International Relations and European Studies,
University of Florence
3 – 5 May 2017

CYBER SECURITY IN THE EUROPEAN UNION

Position paper by

Daigoro Sgarbanti, Fabio Seferi, Greta Faieta, Luca Papini, Morgana Federica Signorini, Pia Dittmar, Remy Gendraud, Sebastiao Trigoso, Valentina Roselli
(University of Florence, Italy)

Daigoro Sgarbanti daigorosgarbanti@yahoo.it
Fabio Seferi Fabio.seferi@stud.unifi.it
Greta Faieta gretafaieta94@gmail.com
Luca Papini luca.papini2@stud.unifi.it
Morgana Federica Signorini morganafedericasignorini@gmail.com
Pia Dittmar pia.dittmar@outlook.fr
Remy Gendraud remy.gendraud@hotmail.fr
Sebastiao Trigoso sebastiaotrigoso@hotmail.com
Valentina Roselli valentina.roselli@stud.unifi.it

Introduction

As delegates of Italy, we would like to start our discussion on the EU crisis talking about a very recent and important issue, giving some personal suggestions in the field of cyber security. Before presenting our opinion on the implementation of cyber security measures in the EU we would like to start with a brief introduction about what is cyber security, why we talk about it and what are the threats. We will also shortly talk about projects and how cyber security is tackled in the EU. This introduction is necessary because of the complexity of the issue and we hope to provide some basic notions to those who haven't dealt with the topic yet in order to stimulate the conversation after.

First of all, we agree that the basic definition of cyber security is "the body of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorized access". We would like to remind that computer technology and the Internet initially were invented for military actions and there was no intention to extend the use of it in the civil society at the beginning. This issue is important to remark because today we are in a sort of "cyber war". We are saying "cyber war" because it's unquestionable that who gains information gains power and today all the information we need are on the Internet.

Today, cyber space is a sort of parallel world in which there are no rules and no control by a superior authority and in the meantime, it is the place where we share our whole life.

Just think that 315 million Europeans are using the Internet every day. Their activities cross all areas of digital society: from e-commerce to finance, from energy to smart mobility. Today we can find and do everything on the Internet. We can search for specific news or information, we can listen to music and watch movies from everywhere. We can even find a partner and stay in touch with persons in every part of the world in every moment. Thus, we can say that the Internet is the backbone of our entire society.

The Internet's impact became increasingly stronger and now we all are its "victims". Relying heavily on the Internet increases the impact that cyber incidents could have on our lives because they could endanger or disrupt essential services connected to healthcare, water, energy and transports.

It is simple to understand why today we want to talk about cyber security. As we said before, we can be seen as "victims" because we all use the cyber space and we manage our everyday life with the help and necessity of the Internet. We move money, search persons, contact people, we make our sensitive data available on the Internet.

We can say that who controls the Internet controls the world. Fortunately, nobody controls the Internet yet but this does not mean that there are no people using cyber space to threaten someone else. All this information that we make available in this space can be stolen by someone else. We must know that cyber threats and cybercrime today cost the EU Member States €265 billion per year.

Hence, cyber security becomes a very important issue in today's life. While being fortunate that there is no one controlling the cyber space, we are also unfortunate because

every one of us is exposed to the threats due to a lack of an authority. Cyber space can be seen as a State without the State, a place in which order and rules are absent.

Probably the biggest issue related to cyber security is that even if we find a way to defend people, industry, governments etc. the threats are too many and they come from everywhere and they are steadily increasing every day. As the experts in security say, "threats accumulate, which means that to the old threats we add the new threats and not that the new ones replace the old ones".

The issue of cyber security is very important for us because dealing with cyber means dealing with a common problem of every single person from Italy to France, from Latvia to Hungary and so on. In the EU, we have a big issue in common and we have to find a common way to deal with it. Given the importance of cyber security, an increase of common actions to deal with the threats can be the right way to relight the spirit of community and integration that characterized the EU until now.

EU strategies

Now we would like to explain briefly what the EU did until today to understand better what is done and what is has to be done. The overall strategic framework on countering cyber threats and cyberterrorism relies on three fundamental instruments:

1)***Cyber security Strategy of the European Union (February 7th, 2013)***

In order to outline an efficient strategy for cyber security and since the core values of the EU apply, similarly to the digital world as to the physical world, some basic principles and values must be granted:

a) fundamental rights, personal data, privacy and freedom of expression;

b) access for all;

c) democratic and efficient multi stake-holder governance;

d) shared responsibility.

The strategy's aims are mainly the following:

a) Achieving cyber resilience

b) Drastically reducing cybercrime

c) Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)

d) Develop the industrial and technological resources for cyber security

e) Establish a coherent international cyberspace policy for the European Union and promote core EU values

The Directive 40/2013 EU, starting from these points, sets a range of articles in order to ensure the proper application of the principles stated before into the framework of the safeguards of the information networks. However, the approach used by the Commission highly relays on the role of the Member States in most of the issues taken into account. Member States are called up both to legislate and to control the application of every article settled into the Directive.

In this framework of thought the EU institutions see themselves more as a coordinator of the policies on cyber security than a direct ruler.

2)***European Agenda on Security (April 28th, 2015)***

This agenda prioritizes certain issues, which share a common degree of urgency, of a strong cross-border dimension, and of a cross-sectional nature. These issues are terrorism, organised crime and cybercrime. All actors involved in tackling these issues have to work together, in respect of 5 key principles:

a) full compliance with fundamental rights;

b) transparency, accountability and democratic control (in order to ensure citizens' confidence and trust);

c) better application of existing EU rules and harmonization with new instruments;

d) joined-up inter-agency and cross-sectorial approach;

e) bringing together of all internal and external dimensions of security (in order to provide an organic approach).

Another fundamental point is the cooperation among different actions (EU institutions and agencies, Member States, etc.) while strengthening the pillars of EU action by using a certain set of tools:

a) better information exchange;

b) increased operational cooperation;

c) Supporting action: training, funding, research and innovation.

3)***Directive on security of network and information systems (the NIS Directive) (adopted by the European Parliament on July 6th, 2016)***

In order to improve the functioning of the internal market and to strengthen Europe 's cyber resilience, this Directive aims at laying down some measures so as to achieve a high common level of network and information systems (NISs) security within the European Union.

Our Proposals

Considering all that has been said above, it becomes clear that more public investment in the digital area is strongly needed at the European level. European countries are severely undeveloped in an area that is changing incredibly fast. In order to get up to speed, European public authorities must be involved massively. This can only be implemented by creating several measures that need to be coordinated, to address the issues of our digital lives in an effective way. We have to understand that merely spending money is not the key to respond to this burning issue, it is the coordination of quality policies that are both really thorough and adaptive.

Therefore, we propose to set a very clear objective: to reach a level in our society in which we have a deep understanding and thus an overall control of our cyber dimension. And like every area of our social life, it has to be safe to flourish, and it would be way more able to do so if the European Union was accountable for it.

The first step towards this goal is of political nature: we need to have a clear, defined and coordinated agenda and budget for these issues. Today, as we have previously shown, cyber-security is addressed by a very complex apparel made of several institutions, at the European level, the national level, and the civil level, and most of them are multi-tasking and they are not focusing their entire attention on cyber-threats. The decision-making process in this area is problematic, time-consuming and often ends up with compromises that do not match this importance of the threat, or that are already obsolete because the issue has already evolved. Simplification and direct action are the keys to fix these inefficiencies. We are aware that having all Member States to agree on this is arduous, but it is also crucial to be coherent and reactive.

The second axe that must be developed is research. This issue is highly technical: The Internet is a totally autonomous and expansive environment, it is a fantastic area of freedom and creativity, it is a world of unlimited opportunities, but the public institutions have barely started to scratch the surface of its understanding. Therefore, we are barely able to protect ourselves and to deal with the threats day-by-day, and huge inequalities remain. We need to be able to understand what the future threats could be, to predict them and also to fight back. This is why we propose to create excellence research centres in the field of cyber-security, in order to attract the best experts and to give them the means to help and protect us. The outcomes of this research need to be applied to concrete situations. This can also be a way to reduce our dependency on foreign products, coming mainly from the USA.

However, since the public sector is not updated as it should, we need to cooperate with private companies, who are more advanced on these issues. Private companies have already started to invest massively since cyber-security is also an economic issue, so everyone is a potential target for a hack, and States have not been able to protect them effectively. Start-ups are blooming all over the world, hiring the best experts to protect private data. They have been able to do it faster and better than both the States and the European Union because they have been acting on these threats right when they appeared and they have attracted the best by offering them higher salaries. If we want to cooperate with the private sector, we need to shape the market with conditions that favour competition and investment. And the European level is the most efficient level to do so. Moreover, by keeping this field competitive, although still regulated by the European

Union, we would encourage all players to keep innovating. Thanks to this, we would have better tools, faster and potentially for lower costs.

And in this spirit of more cooperation and more public investment in the digital field, we think that the relationship between the sector should be reshaped in an innovative way. A good example that could be applied to the European level comes from Denmark. Last February, the Danish foreign minister has announced the creation of a "digital ambassador", who works exclusively with the transnational digital giants of "GAFA": Google, Amazon, Facebook, Apple. This is an ingenious measure, that could be going in the right direction in order to prevent possible threats coming from the private field. The policies we need to implement to keep us cyber-secure won't be effective unless we have an open and cooperative dialogue with those who hold the data that is being targeted. So far, the relationship between the EU and GAFA has been tense, mostly made of restraining policies and judgements, fees and the refusal to pay them. But these companies are a part of our lives, influencing many daily actions.

Private companies are not the only actors playing in this competitive field nor the only possible source of threat. The European Union also has to deal with great powers, like Russia, China or the United States.

It also must be taken into account that if one Member State is under threat, the whole Union is under threat. This stance carries important implications. In the process of reaching the abovementioned goal, which is making the European Union a highly innovative and research-leading environment for technological advancement, it is important to deepen the level of integration between the Member States of the Union, for several reasons.

The first is that single Member States more than others have already done significant progress in the field; these progresses can be shared throughout, and thus bring an advantage to, the whole Union. For this purpose, a stable and direct channel of communication must be established across the Union, through which best practices can be spread.

That will be the first step towards the objective that all Member States first reach, and consequently maintain, the same level of advancement and competence in the field: an advanced and secure environment must be homogeneous in all its components, in order not to have any vulnerabilities. Thus, training should be provided to all Member States; the training should include both theoretical and practical information on all aspects of cyber security, such as what precautions must be taken for prevention of threats, how to better implement high security standards, and how to manage attacks, if and when they occur.

Defining the level to be reached must be done by the Member States collectively and must collectively apply to all of them. In this process of establishing standards, it is important to keep into consideration that certain Member States are more advanced than others; therefore, the standard should be adjusted to the higher already existing inside the Union. As a consequence, each Member State would have a different starting point, and would thus require different actions and a different amount of time to reach the common goals; hence, appropriate assistance has to be provided in each case.

Single high standards apply to different, crucial fields. First, key infrastructures must be taken into consideration: relevant issues that must be regulated are for example the materials used for building infrastructure, their constant maintenance and potential upgrade, their control. If infrastructure in one Member State is open to attack, that could lead to disruption across the European Union, or it could grant access to information sensible for the whole Union. Information is a second matter of great importance and controversy. Indeed, sharing information between Member States is clearly essential: discrepancy of information across the Union could lead to misevaluation of potential threats. However, sharing sensible information is a delicate issue to tackle, not merely for cyber-security, but for all security related fields, as it is linked to one of the core components of state sovereignty. Nonetheless, given today's environment, it is unavoidable, even if it is a practice that Member States will be reluctant to accept. If common high standards for security issues are set, this process will be facilitated, as Member States will feel reassured that sensible information can be handled properly by the European Union. In this framework, another issue that must be considered is the status of former hackers and the eventuality of recruiting them. It is a delicate topic and it cannot be assessed appropriately in this space; one thing can be affirmed, that there cannot be multiple regulations on the matter across the European Union. That could possibly create tension, ambiguity, and unwillingness to cooperate.

If having a deeper cooperation proves effective in this field, this method can, and should, be applied to other central areas of the European Union as well. Indeed, if the EU reaches a more solid background in all subjects it deals with, that can, in our opinion, help to find solutions to many of the problems inside the Union; cyber-security is not the only area we are late on. One important part of this strategy is the creation of a single agency responsible for a specific topic. In the case of cyber-security, a good starting point can be the European Union Agency for Network and Information Security (ENISA), that should however be provided with more powers, because at the moment ENISA only deals with connecting information on cyber-security data of the Member States. The main problem is that national Governments are reluctant to share information connected to security issues; this tendency can be diminished if all Member States are willing to be more transparent with each other (not with the public) on their actions. ENISA could be the tool through which trust can be created, if certain changes are applied.

As a first step to create trust, experts can be appointed by each Country, so that every Member State is perfectly informed at all times on what is being done. The team of experts will work together aiming to reinforce the integration and to create a solid bridge between national agencies and the European one, so that their work is coordinated. As we said above, it is crucial to know how intelligence agencies of each country will use sensible information or tools, such as new software's programs, developed by the research field, that should consequently be closely linked with ENISA.

Since this agency would deal with security problems, it should be put under the control of the European Union External Action Service (EEAS), currently led by the High Representative Federica Mogherini. Having to answer to the European Commission, the European Parliament and the European Council at the same time, this stratagem could make it easier to be accepted by national governments, as they have some control through the European Council, and also by the European people, thanks to the democratic representation in the European Parliament.

There is, however, a very important limitation to the last point raised; and that is that the European Parliament cannot fully play its democratic role because of the incomplete, incoherent and inadequate institutional construction of the Union in general. This matter is obviously too broad to properly be assessed in this paper. However, the specific issue of cyber-security as we have explained it in this paper can be taken as an example of the concept that only after implementing broad reforms that point at further integration, the European Union will be able to a) be a proper democracy and b) effectively respond to problems. Since the Internet is a pervasive tool, which grants those who use it a great and globally influencing power, the European Union needs a pervasive strategy, in order to not be damaged by external threats.

This position paper was written by Rémy Gendraud, Morgana Federica Signorini, Greta Faieta, Fabio Seferi, Pia Dittmar, Daigoro Sgarbanti, Valentina Roselli, Sebastião Trigoso, Luca Papini.